



U.S. General Services Administration

Cyber Technical Support Services

A Procurement by the U.S. General Services Administration (GSA)  
on behalf of the Department of Homeland Security

Solicitation/GSA ITSS Number: ID08180053  
Contract/Task Order Number: TBD

This requirement is being solicited as a Task Order under the  
VETS 2 Government-Wide Acquisition Contract (GWAC)

U.S. General Services Administration  
Federal Acquisition Service, Office of Assisted Acquisitions  
Rocky Mountain Region 8

Proposal Due Date: May 23, 2019 at 1:00 p.m. Mountain Time

## 1.0. VETS 2 TASK ORDER INFORMATION

**1.1. NAICS Code:** The principal nature of the requirements described in this solicitation is consistent with services performed by industries in the 541512 “Computer System Design Services).”

**1.2. Product Service Code (PSC):** Product Service Code R499 “Other Professional Services.”

**1.3. Type of Contract:** This task order will include both Firm Fixed Price (FFP) and Time and Materials (T&M) CLINs.

**1.4. Type of Services:** This task order will involve commercial non-personal professional services.

**1.5. Security Clearances:** See Attachment 1 – Performance Work Statement

**1.6. Performance Location(s):** See Attachment 1 – Performance Work Statement

**1.7. Period of Performance:** The estimated period of performance for this effort includes a 12-month base period and four 12-month option periods as outlined below.

Base Period:	July 1, 2019 – June 30, 2020
Option Period 1:	July 1, 2020 – June 30, 2021
Option Period 2:	July 1, 2021 – June 30, 2022
Option Period 3:	July 1, 2022 – June 30, 2023
Option Period 4:	July 1, 2023 – June 30, 2024

## 2.0 ROLES AND RESPONSIBILITIES

Identification of all government personnel, including their specific roles and responsibilities:

### 2.1 Contracting Officer

Brandy Massingale, GSA FAS  
Telephone Number: (303) 518-8762  
Electronic Mail: [Brandy.Massingale@gsa.gov](mailto:Brandy.Massingale@gsa.gov)

*Responsibility for contracting activities rests solely with the Government Contracting Officer. No conversation, recommendations, or direction, whether given directly by, or implied by Government personnel, that will affect the scope, schedule, or price of the program covered by this solicitation or any resulting contract, shall be acted upon by the Contractor unless specifically approved by the Government Contracting Officer. In the absence of the assigned CO, any GSA Region 8 CO may fill in and has full authority to act on this task order.*

### 2.2 Contracting Specialist

David Shamburger, GSA FAS  
Telephone Number: 720-616-2183  
Electronic Mail: [David.Shamburger@gsa.gov](mailto:David.Shamburger@gsa.gov)

*As a member of the contract administration team, the contract specialist will be responsible for working in concert with the Contracting Officer while performing post award administrative functions and certain assigned pre-award functions.*

### **2.3 Contracting Officer's Representative (COR)**

TBD, DHS  
Telephone Number: TBD  
Electronic Mail: TBD

#### **CONTRACTING OFFICER'S REPRESENTATIVE (DEC 1991)**

(a) Definition. "Contracting officer's representative" means an individual designated in accordance with subsection 201.602-2 of the Defense Federal Acquisition Regulation Supplement and authorized in writing by the contracting officer to perform specific technical or administrative functions.

(b) If the Contracting Officer designates a contracting officer's representative (COR), the Contractor will receive a copy of the written designation. It will specify the extent of the COR's authority to act on behalf of the contracting officer. The COR is not authorized to make any commitments or changes that will affect price, quality, quantity, delivery, or any other term or condition of the contract.

(End of clause)

### **3.0. CONTRACT LINE ITEMS (CLINS) AND CONTRACT TYPE BY CLIN**

See Attachment 2 – Price Schedule

### **4.0. DESCRIPTION OF SERVICES/SCOPE OF WORK**

See Attachment 1 – Performance Work Statement (PWS)

### **5.0. INVOICING INSTRUCTIONS**

In order to allow effective payment management, the contractor shall follow all instructions. Failure to follow invoice submission instructions or invoice requirements may result in delay of payment or rejection of the contractor's invoice.

#### **5.1 Invoice Submission**

The Contractor is required to submit invoices according to block 24 of the GSA Form 300 or Block 18a of the Form 1449.

This electronic invoicing is in lieu of submission via U.S. Mail. Hard copy invoices will not be accepted. The website above provides registration/password instructions. Questions can be directed to GSA Finance Customer Support at FW-ClientServices@GSA.Gov or call (800) 676-3690.

In addition, the Contractor is required to upload a copy of its invoice, including all backup documentation into ITSS to facilitate prompt payment. The contractor shall provide invoice backup data in accordance with section 5.2 Invoice Requirements.

ITSS is GSA FAS's business systems portal. The invoice and ITSS process/registration shall be required for proper invoice submission to GSA.

## 5.2 Invoice Requirements

Invoices shall be submitted in accordance with the Price Schedule described in Attachment 2. All invoices shall identify the specific contract line item number (CLIN), description of related task as stated in the scope of work of this task order, the billing rate and any applicable units executed. Invoices shall be submitted on an individual basis for requirements as defined in the PWS. Invoices shall be submitted on a monthly basis and are required to be submitted in a timely manner. Invoices that do not meet the minimum requirements shall be rejected.

(a) Invoices shall be submitted as an original only, unless otherwise specified, to the designated billing office specified in this order.

(b) Invoices must include the Accounting Control Transaction (ACT) number provided in the order.

(c) In addition to the requirements for a proper invoice specified in the Prompt Payment clause of this contract, the following information or documentation must be submitted with each invoice:

<b>GSA Contract Number:</b>	To be provided at award
<b>Task Order Number:</b>	To be provided at award
<b>ITSS Project Number:</b>	ID08180053
<b>/ACT Number:</b>	To be provided at award
<b>Project Title:</b>	CDM Cyber Technical Support Services
<b>Description:</b>	Task #, CLIN #, PoP

(d) GSA IT-Solutions Shop (ITSS) includes input fields such as invoice number, POC information for who submitted the invoice. Contractor shall include backup information for any subcontracting in spreadsheet form identifying the dollar amount of invoices submitted that were subcontracted and how many of those dollars were subcontracted to small business and any other socioeconomic program under FAR Part 19.

### 5.2.1 Time and Material (T&M) Invoice Requirements (for LABOR)

The contractor may invoice monthly on the basis of cost incurred for the T&M CLINs. The invoice shall include the PoP covered by the invoice and the CLIN number and title. All hours and costs shall be reported by CLIN element. The contractor shall provide supporting information in spreadsheet form. The listing shall include separate columns and totals for the current invoice period and the project to date. The spreadsheet shall include the following detailed information:

1. Employee name (current and past employees)
2. Employee Company
3. Employee company labor category
4. Employee labor category
5. Monthly and total cumulative hours worked
6. Corresponding ceiling rate
7. Cost incurred not billed

### **5.2.2 TRAVEL Invoice Requirements**

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the Federal Travel Regulation (FTR). The invoice shall include the PoP covered by the invoice, the CLIN number and title. As supporting information separate worksheets, in Microsoft (MS) Excel format, shall be submitted for travel.

Total Travel: This spreadsheet shall identify all cumulative travel costs billed against the travel CLIN with a column to identify the total amount billed in support of Task CLINs. The current invoice period's travel details shall include separate columns and totals and include the following:

1. Travel Authorization Request identifier
2. Date COR approved travel
3. Current invoice period
4. Names of persons traveling
5. Number of travel days
6. Dates of travel
7. Number of days per diem charged
8. Per diem rate used
9. Total per diem charged
10. Airfare Cost
11. Rental Car Cost
12. Lodging Cost
13. Total charges
14. Explanation of variances exceeding 10% of the approved versus actual costs

\* Any Misc. additional costs shall be broken out into separate columns.

### **6.3.4 OTHER DIRECT COSTS (ODCs)**

The contractor may invoice monthly on the basis of cost incurred for the ODC CLINs. The invoice shall include the PoP covered by the invoice and the CLIN number and title. In addition, the contractor shall provide the following supporting information for each invoice submitted, as applicable. Spreadsheet submissions, in MS Excel format, are required.

1. ODCs purchased
2. Date delivery accepted by the Government
3. Project-to-date totals for ODCCLINs
4. Remaining balance of ODC CLINs

## **6.0. Solicitation Provisions and TASK ORDER Clauses**

All Applicable and Required provisions/clauses set forth in the VETS 2 GWAC shall automatically flow down to this task order. Representation and Certification Provisions from the VETS 2 GWAC contract automatically flow down to all task orders.

### **6.1. Additional FAR and Agency-Specific Task Order Provisions/Clauses**

The following additional provisions and clauses apply to this task order:

DHS Class HSAM Deviation, Limitation of Government's Obligation shall be included at award in order to allow the Government to incrementally fund the Fixed-Price and T&M CLINs.

HSAR 3052.204-71 Contractor Employee Access (SEP 2012)

HSAR 3052.204-71 Contractor Employee Access Alternate I (SEP 2012)

The following clauses are hereby incorporated into the task order and are provided in full text:

#### **FAR 52.217-8 – Option to Extend Services (NOV 1999)**

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor before expiration of the contract period.

(End of clause)

#### **FAR 52.217-9 – Option to Extend the Term of the Contract (MAR 2000)**

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days of contract expiration; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 calendar days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months.

(End of clause)

#### **HSAR 3052.204-70 Security requirements for unclassified technology resources. (JUN 2006)**

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(End of clause)

## **7.0. PROPOSAL PREPARATION AND SUBMISSION**

### **7.1 Solicitation Closing Date and Time:**

Proposals should be prepared in accordance with the VETS 2 contract and shall explicitly cite their VETS 2 contract number. Offeror proposals are due on May 23, 2019 at **1:00 pm**

**Mountain Time (MT)**. The proposal shall be submitted in GSA's eBuy with attachments on or before the proposal submission deadline. GSA's eBuy transfers offeror proposals directly to the

ITSS Portal automatically. To ensure proper delivery of the proposal, offerors should ensure their Company and POC are the registered in ITSS under the VETS 2 Contract.

Further information on submission of quotations is provided throughout this document. Vendors shall review the submittal requirements for each factor below.

**7.2 Solicitation Questions and Answers:** Questions shall be submitted using the Solicitation Attachment 5 spreadsheet to [Brandy.Massingale@gsa.gov](mailto:Brandy.Massingale@gsa.gov) and [David.Shamburger@gsa.gov](mailto:David.Shamburger@gsa.gov) by **May 6, 2019 at 1:00 pm Mountain Time**. The Government reserves the right to not answer questions submitted after this time. The questions received and Government responses will be provided to all contractors. Questions will not be addressed orally.

### **7.3 Proposal Format:**

The Non-Price Volume of the proposal shall be limited to 7 pages; however, Key Personnel resumes, the Attachment 3 – Relevant Experience Data Sheet(s), the Contract Performance Assessment Reporting System (CPARS) evaluation report(s), and any table of contents or cover pages are not included as part of the page limit. The Price Volume of the proposal is not subject to page limitations. Submission of a proposal represents agreement to all solicitation requirements, including terms and conditions, and technical requirements. Any exceptions or assumptions must be clearly identified in the Contractor's Price Volume.

## **8.0 EVALUATION AND AWARD**

To ensure timely and equitable evaluation of proposals, Contractor (defined as the entity submitting the proposal) must follow the instructions contained herein. Proposals not conforming to this solicitation may be determined as being unacceptable, thereby eliminating them from further consideration. The Government reserves the right, at its sole discretion, to hold exchanges, clarify any proposal item, or discuss any other topic at any other time with a single contractor or other contractors as deemed appropriate by the Contracting Officer.

This procurement will be conducted in accordance with the terms and conditions of the Vets 2 GWAC and FAR16.505. The task order will be awarded to the Contractor whose proposal represents the best value to the Government considering the price and non-price factors. The Government may award to other than the lowest price proposal or other than the highest technically rated proposal. The non-price factors are of equal importance to each other, and when combined, are significantly more important than price.

### **Minimum Requirement**

Contractors shall complete and submit Attachment 6 - DD Form 254, on or before **May 6, 2019 at 1:00pm MT** to David Shamburger at [david.shamburger@gsa.gov](mailto:david.shamburger@gsa.gov) and Brandy Massingale at [brandy.massingale@gsa.gov](mailto:brandy.massingale@gsa.gov). No late or incomplete submittals shall be accepted.

The completed DD Form 254 will be used for verification of a TOP SECRET facility clearance by the Government. The Government will confirm the vendor possess the required TOP SECRET facility clearance. Failure by the Contractor to submit the required DD Form 254 by the due date; or submission of an incomplete form; or the lack of a verifiable TOP SECRET Facility Clearance will result in a "no-go" rating, and Contractor's quote will no longer be eligible for consideration.



## 8.1 Non-Price Factors

### Factor 1 – Staffing Plan

Contractor must submit a staffing plan to demonstrate its ability to satisfy the requirements identified in the PWS. The staffing plan must include, at a minimum, the following elements:

- a) A narrative addressing the Contractor's staffing approach specific to this requirement, which, at a minimum, must include its plan to recruit and retain personnel to provide uninterrupted services. Offeror shall address their plan to staff the requirement during the (2) month transition period when considering the DHS Entrance on Duty (EOD) process.
- b) A staffing matrix which details the qualifications of all the proposed labor categories.
- c) Resumes for the Key Personnel positions, outlining the education, experience, and clearance qualifications.

#### Basis of Evaluation:

The Government will evaluate the Contractor's staffing plan to determine whether the proposal demonstrates a sound approach to recruit and retain personnel, as well as its understanding of requirements outlined in the PWS, including the DHS EOD process. A staffing plan which mitigates potential risk of a lengthy clearance process may be rated more favorably. The staffing plan will also be evaluated to determine whether the staffing matrix reflects appropriate qualifications to provide quality services based on the Contractor's proposed labor categories. Staffing plans which present less risk may be rated more favorably. Proposed Key Personnel staff which exceed the minimum education and/or experience requirements may also be rated more favorably. In regards to the Lead Capability Subject Matter Expert position, if the proposed individual possesses experience in market leading tools or products associated with Continuous Diagnostics and Mitigation (CDM) that may also lead to a more favorable rating.

### Factor 2 – Relevant Experience

This factor considers the Offeror's relevant experience as a prime or subcontractor performing similar contract/TO work for at least one (1) year within the last three (3) years prior to the RFP issuance date. Offeror shall submit at least one (1), but no more than three (3) examples using Attachment 3 – Relevant Experience Data Sheet. Offeror shall include at least one (1) contract/TO where they were the prime contractor. Additionally, at least one example shall be of a Federal Government contract or task order issued against a Federal Government contract.

Each similar contract/TO must contain the following minimum characteristics:

- a) A main objective of providing cyber security professional support services;
- b) Total value of approximately \$5M per year; and
- c) Additionally, the examples provided must collectively demonstrate experience in ALL the following Task areas:

1. Task 1 – Project Management (PWS 4.1)
2. Task 2 – Engineering Support (PWS 4.2)
3. Task 3 – Dashboard Operations (PWS 4.3)
4. Task 4 – Agency Readiness Assessment and Requirements Package Support (PWS 4.4)
5. Task 5 – Requirements Development and Management Support (PWS 4.5)
6. Task 6 – Test and Evaluation Support (PWS 4.6)
7. Task 7 – Cybersecurity Tool Management (PWS 4.7)

### **Basis of Evaluation:**

Offeror must demonstrate its experience as a Prime or Subcontractor performing at least one (1) Similar Contract/TO for at least one (1) year within the last three (3) years prior to the RFP date. Offerors providing one relevant experience project which meets the definition of Similar Contract/TO (a, b, and all tasks listed in c) may be rated more favorably. Offerors providing relevant experience project(s) which meets the definition of Similar Contract/TO (a, b, and all tasks listed in c) and demonstrates additional experience relevant to the tasks outlined in the PWS may also be rated more favorably. Finally, offerors demonstrating more experience as a Prime may also be rated more favorably.

### **Factor 3 – Past Performance**

For each project submitted in response to Factor 2 – Relevant Experience, which meets the definition of “Similar Contract/TO work,” the Government will evaluate the offeror’s past performance on that Similar Contract/TO.

If a completed Contract Performance Assessment Reporting System (CPARS) evaluation report is available for each Similar Contract/TO performed by the offeror as a prime contractor within the last three years prior to issuance of the RFP, then the Offeror should submit the CPARS report with its offer. If a CPARS evaluation report is not available, offeror shall have a Government Point of Contact (.gov email address) submit a completely filled out Attachment 4 - Past Performance Questionnaire for each project submitted in response to Factor 2 by the initial proposal closing date and time to [david.shamburger@gsa.gov](mailto:david.shamburger@gsa.gov) at [brandy.massingale@gsa.gov](mailto:brandy.massingale@gsa.gov).

### **Basis of Evaluation:**

The Government will consider, for each of the Similar Contract/TOs submitted and performed by the offeror as a prime contractor (1) (if available) the completed CPARS Evaluation Report submitted by the offeror by the deadline for submission of offers in response to this RFP; or (2) the information provided to the Government with in Attachment 4 – Past Performance Questionnaire; In addition, the Government may also consider contractor past performance information it obtains on its own from other sources regarding the offeror’s past performance as a prime contractor performing Similar Contract/TO work on contracts other than those submitted for Factor 2.

The Government may use a variety of methods to obtain past performance information including but not limited to personal knowledge of the offeror’s performance, information contained in the Past Performance Information Retrieval System (PPIRS), or other information received.

Offerors which received ratings above Satisfactory, may be rated more favorably.

## **8.2 Price Factor**

Utilizing Attachment 2 – Price Schedule, Contractor shall submit a price proposal for all work identified in the PWS. Travel (if needed and authorized by the Government) will be reimbursed at actual costs in accordance with the limitations set forth in FAR 31.205-46.

### **Basis for Evaluation:**

The Government will evaluate Contractor prices utilizing any price analysis technique(s). The Government will evaluate the Contractor's price proposal by evaluating the total overall price, base and all option periods. Additionally, as part of its price evaluation, the Government will evaluate its option to extend services (see, FAR Clause 52.217-8) by adding one-half of the Contractor's price for Option Period 4 to its total price. Thus, the Contractor's total evaluated price will include the base period, option periods 2 through 4, and the six month extension option. Evaluation of the option periods and the six month extension option does not obligate the Government to exercise either. Proposals that are unbalanced or unreasonable may be rejected as unacceptable and ineligible for award.

## **9.0 ATTACHMENTS**

Attachment 1 – Performance Work Statement  
Attachment 2 – Price Schedule  
Attachment 3 – Relevant Experience Data Sheet  
Attachment 4 – Past Performance Questionnaire  
Attachment 5 – Solicitation Questions and Answers  
Attachment 6 – DD Form 254  
Attachment 7 – Draft RFP Q & A Spreadsheet (For informational purposes only)

# **Continuous Diagnostics and Mitigation (CDM) Cyber Technical Support Services (CTSS) Performance Work Statement (PWS)**



## **1 PURPOSE**

The purpose of this Task Order (TO) is to provide cybersecurity subject matter expertise (SME) to support the government in conducting effective engineering, requirements development and documentation, and technical documentation development and review activities.

## **2 BACKGROUND**

The United States faces increasingly skilled cyber threats that seek to penetrate our government from a number of sources (e.g., outside, inside and within our information technology capabilities). Beyond the potential theft of state secrets, and the loss of proprietary intellectual property, these threats are even thought to pose a national security risk to the United States. The Department of Homeland Security (DHS) operates as a partner with the private sector, law enforcement, intelligence, and military communities providing critical support as part of a national mission to detect, analyze, pursue, and mitigate cyber threats to the United States.

To support the DHS cyber mission, the Cybersecurity and Infrastructure Security Agency (CISA), leads the design, development, deployment, and systems operation and maintenance of cyber security technologies to counter sophisticated cyber adversaries and apply effective risk mitigation strategies to detect and deter these threats. Additionally, NSD in partnership with industry and Federal partners, provides technological innovation and development to promote the overall effectiveness of the cyber security effort.

CISA is responsible for managing the Continuous Diagnostics and Mitigation (CDM) program; a Level 1 Acquisition program. The CDM program is a dynamic approach to fortifying the cybersecurity of Government networks and systems. The cyber landscape in which Federal Agencies operate is constantly changing and dynamic. Threats to the nation's information security continue to evolve and Government leaders recognize the need for a modified approach to protecting our cyber infrastructure. The CDM Program enables DHS, along with Federal Agencies and state, local, regional, and tribal governments, with the ability to enhance and further automate their existing continuous network monitoring capabilities, correlate and analyze critical cybersecurity-related information, and enhance risk-based decision making at the Agency and Federal enterprise level. The CDM Program benefits participating Agencies by helping to identify information security risks on an ongoing basis so that Agencies can rapidly detect and then respond to information security events.

Congress established the CDM program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources. CDM provides Federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

The CDM Program is organized by capabilities as identified below Figure 1: CDM Capabilities .



**Figure 1: CDM Capabilities**

## **2.1 DHS CDM PROGRAM MISSION**

The CDM Program is managed within the DHS Cybersecurity and Infrastructure Security Agency (CISA), responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. The DHS CDM Program mission is to safeguard and secure cyberspace in an environment where the threat of cyber-attack is continuously growing and evolving. The CDM Program defends the United States (U.S.) Federal IT networks from cybersecurity threats by providing continuous monitoring sensors (tools), diagnosis, mitigation tools, and associated services to strengthen the security posture of Government networks. DHS

has been given the authority and Federal funding to implement the CDM Program to ensure that the approach to continuous monitoring is consistent, meets a common set of capabilities, and leverages centralized acquisition to improve the speed of procurement and achieve significant cost savings by consolidating like Federal requirements into “buying groups.”

## 2.2 SCOPE

The scope of this Task Order encompasses SME support for all CDM capabilities (reference section 4.0 of this PWS and **Attachments A and B: CDM Technical Capabilities Requirements Documentation Volume 1 & 2**) as well as architecture planning, engineering, requirements, process management and training support required by the government. Specifically, this includes direct support to PMO leadership and the Requirements and Systems Analysis/Engineering, Development and Integration teams (see Figure 2. CDM organization chart in section 2.1) in the management of ongoing CDM architecture and solution design efforts, tool procurement activities as well as solution implementation and operations. The contractor shall provide the required level of expertise, experience and qualifications associated with CDM capabilities, products and tools listed in subsequent sections and attachments to support PMO requirements. While the type and level of detailed support may vary based on deliverables from ongoing and future CDM development contracts, general expertise and/or support includes, but is not limited to:

- a. HW/SW Asset management
- b. Configuration management
- c. Vulnerability management
- d. Manage Trust in People Granted Access
- e. Security-Related Behavior Management
- f. Credentials and Authentication Management
- g. Manage Privileged Account Access
- h. Network, Physical and Virtual Boundary Protection
- i. Incident response
- j. Security Lifecycle Management
- k. Data Discovery/Classification
- l. Data protection through access control, cryptographic and masking methods
- m. Data Loss Prevention
- n. Data Breach/Spillage Mitigation
- o. Digital and Information Rights Management
- p. Microsegmentation
- q. Cloud and Mobile Device security and management
- r. Creation, development and/or review of technical documentation and materials for the CDM program

- s. Architecture and Top-level requirements development
- t. Engineering test design planning and technical documentation review
- u. Familiarity with NIST 800-53 security controls and their application within federal information systems risk management frameworks
- v. Support functions required to perform the tasks outlined in a through u such as Program Management, Quality Assurance and other administrative functions.

As the CDM programmatic and contractual requirements are dynamic and complex, the contractor shall use strategic vision in addressing contract requirements. This includes, but is not limited to task management, solutions engineering, test and evaluation, risk management, Request for Service (RFS) development and tracking, SELC artifact validation and review, studies and analysis and configuration management.

Performance of this support will be on-site at the government facility and off-site at the contractor facility. The contractor's facility shall be within the Washington DC metro area/NCR and in close proximity to the CDM PMO in Arlington, VA (Ballston area). The contractor shall be required to routinely travel to the to the CDM PMO Arlington, VA (Ballston area) office. The contractor's facility shall include conference and meeting room space and support routine CDM meetings and events. The contractor shall provide support to the above locations during normal operating hours from 0800 to 1700 on a daily basis, five (5) days a week (Monday through Friday).

## 2.2.1 CONTRACTOR ROLES AND RESPONSIBILITIES

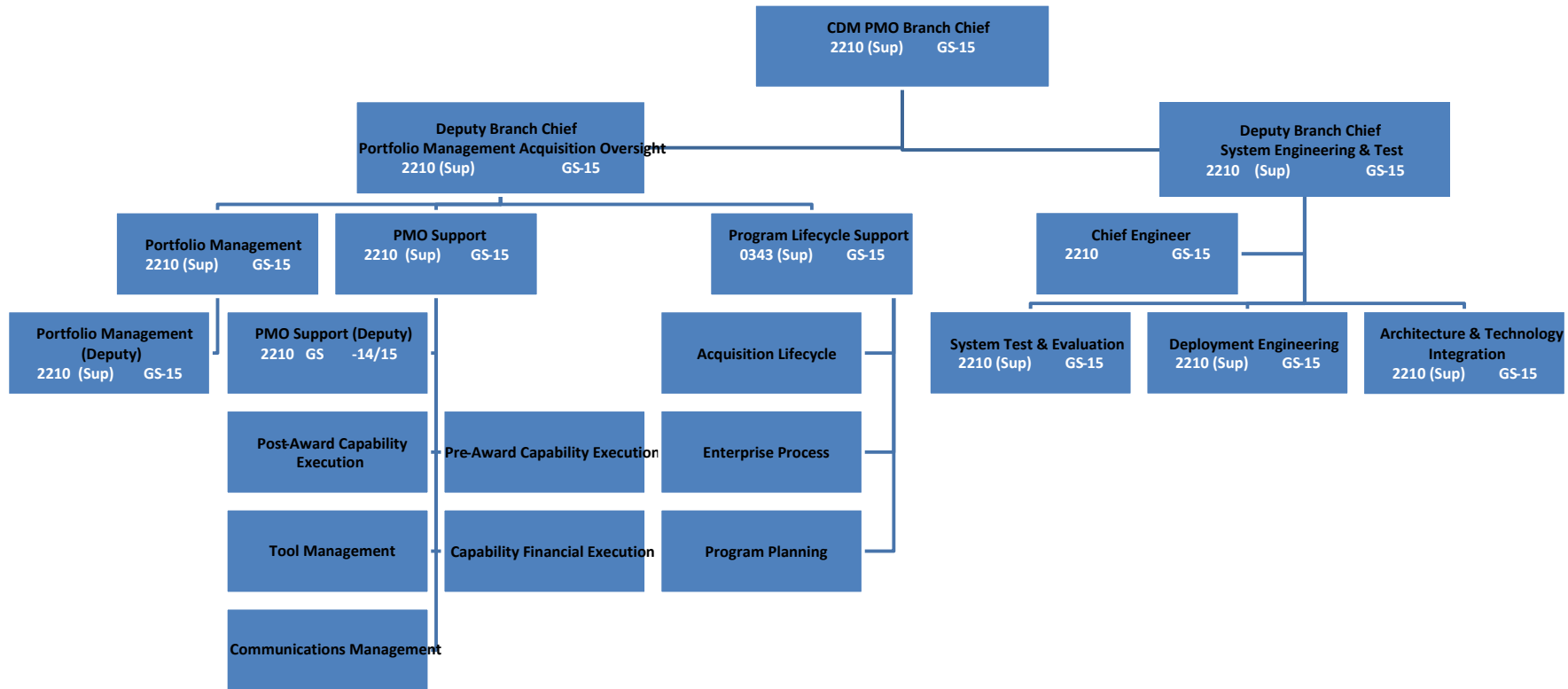
In addition to the SME services to be awarded through this TO, the government will maintain existing contracts and/or award new contracts to support current and future CDM capabilities. The CDM Technical SME support contractor shall be required to work closely with the CDM PMO government team, federal agencies external to DHS (**Attachment C List of Supported Agencies**) and other contractors including CDM DEFEND Integrators and Federally Funded Research and Development Centers (FFRDCs) to help meet program and/or project objectives.

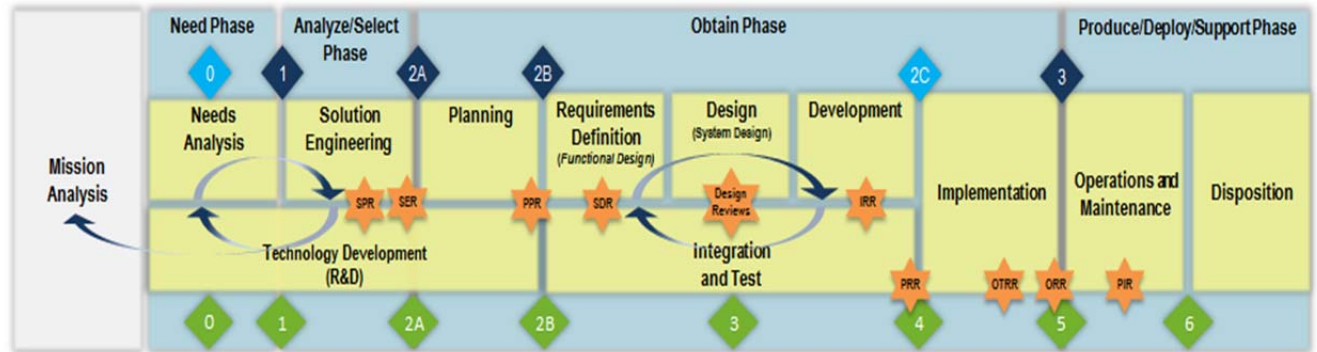
Delineation of contractor roles and responsibilities is critical to the success of the CDM effort (please see Section I for Organizational Conflict of Interest clauses). Figure 2 below provides the current organizational structure of the CDM PMO. Figure 3 depicts the Systems Engineering Life Cycle (SELC) process (**Attachment D DHS SELC Process Overview for more information**). The SELC process includes nine stages and corresponding Systems Engineering Reviews: Solution Engineering, Planning, Requirements Definition, Design, Development, Integration & Test, Implementation, Operations & Maintenance, and Disposition. SELC stage entry and exit criteria completion (as well as technical progress) are validated in the stage










reviews. Solution Engineering focuses on enterprise level activities. The remaining stages address project and system related activities. The contractor shall provide support across all phases of the SELC: including engineering review and SELC stage specific activities as required. The stages and reviews may be repeated by projects and Task Orders during a capability's implementation. These activities and stages may be tailored by the CDM PMO as not all projects or TO efforts will require every stage.

# CDM – PMO (Top Level)





SELC Technical Reviews
• SPR: Study Plan Review
• SER: Solution Engineering Review
• PPR: Project Planning Review
• SDR: System Definition Review
• Design Reviews: Preliminary Design Review and Critical Design Review
• IRR: Integration Readiness Review
• PRR: Production Readiness Review
• OTRR: Operational Test Readiness Review
• ORR: Operational Readiness Review
• PIR: Post Implementation Review

Legend			
• Event-Based SELC Technical Review		• ALF Phase	
• AcquisitionLife Cycle Framework (ALF) Acquisition Decision Event		• SELC Activity	
• ALF Conditional Acquisition Decision Event		• Other DHS Activity	
• Enterprise Architecture Decision			

## TO Tailored SELC

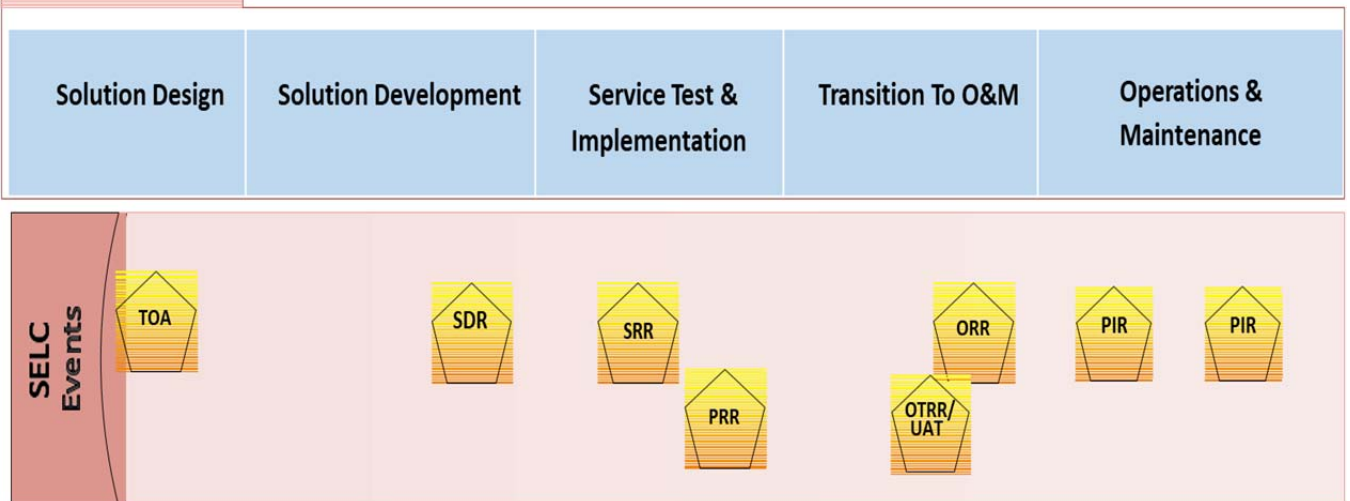


Diagram 5: Tailored DHS SELC Process

<b>SELC Event Legend:</b>
SDR - Solution Design Review
SRR- Solution Readiness Review
PRR - Product Readiness Review
ORR - Operational Readiness Review
UAT – User Acceptance Test Review
OTRR - Operational Test Readiness Review
PIR - Post Implementation Review

### 3.0 CDM PROGRAM CURRENT AND FUTURE STATES

Section 3.0 provides details regarding the CDM architecture and capabilities and is for background and information purposes only.

The CDM program provides tools and services that enable federal and other government IT networks to strengthen the security posture of their cyber networks. DHS works with federal departments and agencies to implement CDM in a consistent manner that demonstrates measureable cybersecurity results and leverages strategic sourcing to achieve cost savings.

CDM enables activities designed to strengthen the cybersecurity posture of the Federal civilian unclassified .gov networks. Specifically, the tools and sensors and associated services benefit the CDM Program by providing the following:

- a. Simplifying the security authorization process by helping to automate security assessments
- b. Continuously monitoring and reporting system security status to Agency cybersecurity personnel via the Agency CDM Dashboard
- c. Providing specific details to help prioritize remediation efforts
- d. Allowing system owners, risk managers, authorizing officials, and other stakeholders to make better risk-management decisions
- e. Automated reporting the security posture of Agency IT assets to the Federal Dashboard, reducing the requirement for manual reporting

The remainder of Section 3.0 summarizes the CDM Current State, CDM Desired Future State, and CDM Technical Capabilities. Where there is a perceived conflict between Section 4.0 and the CDM Technical Capabilities Requirements Documents, Volumes 1 and 2, the CDM Technical Capabilities Requirements Documents will take precedence.

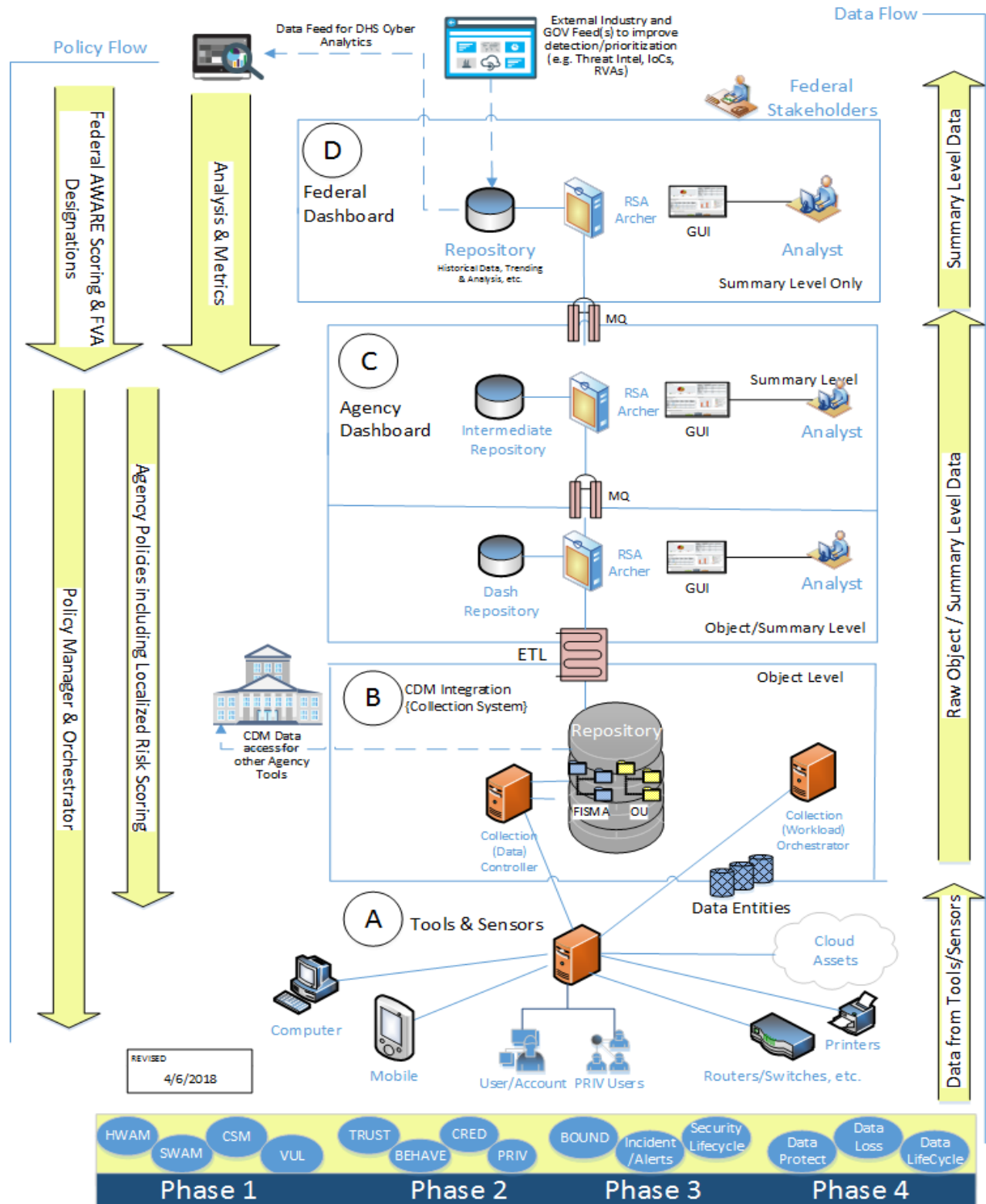
#### 3.1 CDM CURRENT STATE

An Agency-specific CDM solution is currently operating on the Agencies' networks with diverse IT environments. The CDM solutions leverage a similar set of Commercial Off-the-Shelf (COTS) tools. These tools have been reviewed by the DHS CDM Program Office to identify that they meet the capabilities of or in conjunction together meet the requirements specified in CDM Technical Capabilities Requirements Document, Volumes 1 and 2 (**Attachments A and B**). A list of approved CDM Tools is maintained by the DHS CDM Program Office as the Approved Product List (APL), and is located at [www.gsa.gov/CDM](http://www.gsa.gov/CDM).

The CDM system architecture, shown below in Figure 4 – CDM Architecture, illustrates the

CDM Full Operating Capabilities (FOC) vision once it has been implemented within the Agencies.

- a. Area A is the location for tools and sensors that, together, provide the coverage of the CDM Capabilities
- b. Area B is the integration point solution that supports the required operational control points for the CDM Solution
- c. Area C is the Agency CDM Dashboard(s) that integrates into the Agency CDM Solution
- d. Area D is the Federal CDM Dashboard.



IAW tasks listed in Section 4, The Contractor shall support the PMO in managing CDM current solutions through oversight of existing development contracts with other CDM Integrators.

### **3.2 CDM FUTURE STATE**

The CDM solutions at each Agency must meet the operational and functional requirements as detailed in CDM Technical Capabilities Requirements Documents, Volumes 1 and 2 (**Attachments A and B**) for all CDM areas.

The Government requires an integrated solution that includes support for each of the capabilities of the CDM Program. This multi-phase integrated solution will provide a common set of capabilities across the Agencies to fulfill the capabilities of the CDM Program. The Government desires continued enhancement of data aggregation for the Agency dashboards, then integration through the Federal Dashboard to improve the visibility and identification of cyber threats to Federal Networks.

Due to rigid governance structures, diversity of mission, and the interconnectedness of the Agencies' environments, most Agencies have yet to develop an enterprise-class IT solution using modern system development practices. Regardless, the CDM Program has a strong preference for utilizing modern development methodologies including, but not limited to, Agile Scrum, Kanban, or Scaled Agile Framework (SAFe).

The CDM solution provides continued integration, operation, and maintenance of the Agency level CDM Dashboard ensuring that all installed CDM tools and sensors report to the Agency Dashboard as necessary. The Government recognizes that many of the CDM Tools and sensors are able to meet multiple capabilities and therefore any solution must to the maximum extent possible and practicable build off of the existing CDM investments.

As detailed later in Section 4.0 , the contractor shall assist the government in providing cybersecurity and IT subject matter expertise to aid the PMO in developing and maintaining capabilities aligned with CDM future states.

### **3.3 CDM TECHNICAL CAPABILITIES**

As previously depicted, the CDM Program is organized by capabilities (previously referred to as phases), which are not necessarily sequential. Each high level, foundational CDM capability consists of multiple CDM capabilities which are highlighted below. The detailed functional and operational requirements of Asset management and Identity and Access Management capability areas (previously referred to as Phase 1 and 2 respectively) are further described in the CDM Technical Capabilities Requirements Document, Volume 2. Sections 4.3.1 and 4.3.2 provide additional detail for Network Security Management and Data Protection capabilities (previously



referred to as Phase 3 and 4 respectively). As stated in section 2.0 and detailed in section 4.0, the contractor is required to provide the PMO expertise and guidance on the below foundational capabilities:

#### Asset Management

- HWAM – Hardware Asset Management
- SWAM – Software Asset Management
- CSM – Configuration Settings Management
- VUL – Vulnerability Management

#### Identity and Access Management (IAM)

- TRUST – Manage Trust in People Granted Access
- BEHV – Security-Related Behavior Management
- CRED – Credentials and Authentication Management
- PRIV – Manage Privileged Account Access

#### Network Security Management

- BOUND
  - (BOUND-E) Monitor and Manage Cryptographic Mechanisms Controls
    - Cryptography
    - Key Management/Certificate Authority
  - (BOUND-P) Monitor and Manage Physical Access Controls
- Manage Events
  - Incident Response
  - Privacy
  - Contingency Planning
  - Audit and Accountability
  - Ongoing Assessment
- Operate, Monitor and Improve (OMI)
  - Ongoing Authorization
  - System and Information Integrity
  - Risk Assessment
  - Security Assessment and Authorization
- Design and Build-in Security (DBS)
  - DBS Design
  - DBS Development
  - DBS Deployment
  - Supply Chain Risk Management (SCRM)

#### Data centric security and Data Protection Management

- Data Discovery/Classification

- Data Protection
- Data Loss Prevention
- Data Breach/Spillage Mitigation
- Digital Data and Information Rights Management.

### **3.4 CDM Dynamic and Evolving Federal Enterprise Network Defense (DEFEND)**

In January 2013 DHS (operating on behalf of participating Federal Agencies) provided tools/sensors and services to meet Asset Management requirements (previously named Phase 1) of the CDM Program. Beginning in June 2016, DHS provided tools/sensors and services to participating Agencies to meet IAM requirements (previously named Phase 2) of the CDM program. In early 2018, the CDM Program began follow-on efforts to resolve CDM capability gaps, enhance existing CDM capabilities, introduce new CDM capabilities, and provide support to the CDM solutions of participating Agencies leading to a strengthening of their overall cybersecurity posture. The CDM solutions include CDM approved products, configured to reflect the DHS CDM Program priorities and Agency policies as appropriate, that implements a common set of capabilities and enable increased risk-reduction and alignment with Agency risk tolerance. To do this work, the Program established the DEFEND acquisition strategy and utilizes it to execute program capabilities on behalf of Department and Agencies. The CDM program has created Portfolio Teams to support each DEFEND Order consisting of Portfolio Management, Engineering Support, Acquisition and Technical POC, and Test Representative. This Task Order shall support the Portfolio Teams as well as DEFEND activities.

#### **3.4.1 DEFEND REQUEST FOR SERVICE (RFS) PROCESS**

The CDM acquisition strategy required a flexible approach to support the evolving Continuous Diagnostics and Mitigation (CDM) technical capabilities in a rapidly changing cybersecurity environment during the entire life of current and future CDM DEFEND Task Orders (TOs). To support this need, the CDM DEFEND TOs utilizes a RFS process that allows for the iterative execution of requirements to occur throughout the period of performance (PoP) of a CDM DEFEND TO. A RFS can be initiated by an Agency or by the DHS CDM Program Management Office (PMO). This flexibility allows the CDM Program and Agencies to fund and execute support under any CDM DEFEND TO. This support includes all CDM capabilities development or integration as well as expanded services supporting existing tools or products or future capabilities and requirements. The RFS process involves the development of a needs statement and government cost estimate and will require oversight as the DEFEND orders become more mature. The contractor shall support the CDM PMO throughout this process.

## **4.0 TASKS**

The contractor shall provide the support described in the following overarching tasks:

- **Task 1—Provide Project Management**
- **Task 2—Provide Engineering Support**
- **Task 3— Support CDM Program Dashboard Operations**
- **Task 4—Assess Agency Readiness Assessment and RFS Support**
- **Task 5—Provide Requirements Development and Management Support**
- **Task 6—Provide Test and Evaluation Support**
- **Task 7— Perform Approved Product List Administration and Management**

Associated deliverables with the above Task areas are identified throughout Section 2 and a consolidated list is provided in later Sections. The tasks are separated into mandatory and optional categories. The CDM PMO fully expects these annotated task areas to grow during the period of performance. As such, the contractor plan and manage resources accordingly to meet this dynamic requirement. Specific security requirements and expectations of the contractor and any personnel used to support the task areas are contained in **Attachment E** of this PWS.

### **4.1 TASK 1 – PROVIDE PROJECT MANAGEMENT**

The contractor shall provide project management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this PWS. The contractor shall identify a Project Manager (PM) by name who shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO.

The contractor shall use industry-best standards and proven methodologies that ensure all TO activities are identified, documented, and tracked so that the TO can continuously be evaluated and monitored for timely and quality service. The contractor shall notify the Contracting Officer (CO), Contracting Officer's Representative (COR) and the DHS Technical Point of Contact (TPOC) of any technical, financial, personnel, Organizational Conflict of Interest (OCI), or general managerial problems encountered throughout the life of the TO.

The contractor shall facilitate Government and contractor communications and all activities necessary to ensure the accomplishment of timely and effective support, performed in accordance with the requirements contained in this TO.

#### **4.1.1 SUBTASK 1.1 – COORDINATE A PROJECT KICKOFF MEETING**

The contractor shall schedule and coordinate a Project Kick-off Meeting within two (2) weeks after TO award (TOA) in the National Capital Area (NCR) at a location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and logistic issues; travel authorization; and reporting procedures. At a minimum, the attendees shall include key contractor personnel, TPOC, CDM Customer Representatives (CRs), key Government representatives, and the Contracting Officer (CO), and COR. The contractor shall provide a Kick-Off Meeting Agenda (**Deliverable 01**) that will include, but not limited to, the following:

- Introduction of personnel
- Overview of project tasks
- Overview of organization (complexity)
- Schedule (shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each)
- Communication Plan/lines of communication overview (between both contractor and Government)
- Discussion of draft Program Management Plan (PMP)
- Travel notification and processes
- Government-furnished information (GFI)
- Security requirements (Building access, badges, ))
- Invoice procedures
- Monthly meeting dates
- Reporting Requirements, e.g. Monthly Status Report (MSR)
- POCs
- Roles and Responsibilities
- Overview of incoming Transition Plan to include process, timeframes, and status
- Prioritization of contractor activities
- Any initial deliverables
- Other logistic issues
- Quality Control Plan (QCP)
- Sensitivity and protection of information
- Additional issues of concern (Leave/back-up support).

The contractor shall provide a draft copy of the agenda for review and approval by the COR prior to finalizing. The Government will provide the contractor with the number of participants

for the kick-off meeting and the contractor shall provide sufficient copies of the presentation for all present (**Deliverable 02**).

#### **4.1.2 SUBTASK 1.2 – PREPARE MANAGEMENT REPORTS**

##### **MONTHLY STATUS REPORT (MSR)**

The contractor PM shall develop and deliver a MSR (**Deliverable 03**) using Microsoft (MS) Office Suite applications by the tenth (10<sup>th</sup>) of each month or the following business day (if the 10<sup>th</sup> falls on a Saturday or Sunday) via electronic mail (email) to the COR. The report shall briefly summarize, by task, the management and technical work conducted during the month. The contractor shall provide at a minimum the following information:

- Activities during reporting period, by task and Subtask to include: On-going activities, new activities, activities completed, deliverables submitted for that period; and progress to date on all above mentioned activities. Start each section with a brief description of the task.
- Problems and corrective actions taken. Also include issues or concerns that may affect project milestones, personnel, and cost resources and proposed resolutions to address them to include risk mitigation plans.
- Personnel gains, losses and staffing status (upcoming leave, etc.) (LH only).
- Government actions required (deliverables awaiting Government approval, etc.).
- Schedule (from the PMP shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- Summary of trips taken, conferences attended, etc.
- Projected cost of each CLIN broken-down by Task and Subtask for the current month for tracking purposes.
- Financial status including (LH only):
  - Chart reflecting funding and burn rate for the month and cumulative
  - Cumulative invoiced costs for each CLIN and Labor Tasks totals to-date.
- A list of current deliverables and milestones generated from the PMP identifying deliverable due dates. The list shall identify deliverables and milestones submitted for the period by task as well as provide a projection for the following three (3) months.
- Recommendations for change, modifications, or improvements in task or process.

The contractor shall reconcile the MSR with each monthly invoice.

##### **PREPARE TRIP REPORTS**

The Government will identify the need for a Trip Report (if required) when a request for travel is submitted. The contractor shall submit Trip Reports five (5) working days after completion of a trip for all long distance travel (**Deliverable 04**).

The Trip Report will include the following information:

- Personnel traveled

- Dates of travel
- Destination(s)
- Purpose of trip
- Cost of the trip
- Approval authority
- Summary of events, action items and deliverables

The contractor shall keep a historical summary of all long-distance travel, to include, at a minimum, the name of the employee, government approval authority, and location of travel, duration of trip, total cost and purpose.

### **MEETING REPORTS**

The Government will identify the need for a Meeting Report (if required) when a meeting is scheduled. The contractor shall submit Meeting Reports to document results of meetings **(Deliverable 05)** one (1) working day following the completion of each meeting. The Meeting Report will include the following information:

- Meeting attendees and their contact information – at minimum identify organizations represented
- Meeting dates
- Meeting location
- Purpose of meeting
- Summary of events, action items and deliverables

The contractor shall reconcile their Meeting Report with official meeting minutes if published and advise the CDM COR accordingly.

### **PROBLEM NOTIFICATION REPORTS (PNRs)**

The contractor shall file a Problem Notification Report (PNR) one day after the problem is identified **(Deliverable 06)** to notify the COR of TO issues such as potential cost/schedule overruns/impacts, assumptions upon which tasks were based that have changed or were incorrect, etc. The PNR shall be prepared in accordance with the sample provided and include a plan detailing the proposed resolution.

#### **4.1.3 SUBTASK 1.3 – CONVENE IN PROGRESS REVIEWS (IPR)**

The contractor shall conduct formal In Progress Reviews (IPRs) to be held quarterly at the place of performance **(Deliverable 07)**. IPRs shall include the COR, other key Government stakeholders, and additional Government and contractor representatives deemed necessary by the COR. The IPR will provide a forum for Government review of progress, planning, and issues related to the TO. The contractor shall utilize the PMP in their discussion of TO performance. The contractor shall document and email IPR minutes to IPR participant within five (5) business days. IPRs shall include: Schedule by task; previous months activities by task; planned activities for next month by task; issues/actions required by the Government.

#### **4.1.4 SUBTASK 1.4 – PREPARE A PROGRAM MANAGEMENT PLAN (PMP)**

The contractor shall develop and deliver a Draft and Final PMP (**Deliverable 08 and 09**) that is based on the contractor's proposed solution. The contractor shall document all support requirements in the PMP. The PMP shall be automated utilizing software such as MS Project and describe the proposed management approach. The PMP shall cover the entire project and outline the tasks and deliverables necessary to meet the PWS objectives of this RFQ. The PMP shall include milestones, tasks, and subtasks required in this TO. The contractor shall present and brief the draft PMP at the Kick-Off meeting. Following the Kick-Off meeting, the contractor shall revise the PMP to incorporate Government comments. The PMP shall contain, at a minimum, the following for each task:

- All standards followed in support of these requirements.
- A matrix of all deliverables and planned delivery dates.
- Task methodologies.
- Standard Operating Procedures (SOP's) for all tasks.
- A matrix of all personnel (subcontractors and/or consultants) assigned to the program and total aggregate level of effort for all tasks, including position, office location, building access status, and DHS computer equipment (if any).
- Task dependencies and interrelationships.
- Contractor organizational structure.
- Process management and controls.
- Quality control and processes (include the contractor's QCP).
- Any unique hardware and software utilized by the contractor.
- Subcontracting plan, including scope and terms of all active subcontracts (if any).
- POCs.
- General operating procedures for
  - Travel
  - Work hours
  - Leave
  - Deliverables
  - Staff training policies
  - Problem/issue resolution procedures.

The PMP shall contain a separate schedule for each organization area that contains deliverable milestones and deadlines.

The contractor shall incorporate the Government comments into a final PMP no later than thirty (30) days after the kick-off meeting (**see Section 5, Deliverable 9**). Changes to the final program plan may be made with mutual consent of the contractor and the Government.

##### **4.1.4.1 UPDATE THE PROGRAM MANAGEMENT PLAN (PMP)**

The PMP is an evolving document that shall be updated with significant changes as required and at least quarterly at a minimum **(Deliverable 10)**. The contractor shall work from the latest Government approved version of the PMP.

#### **4.1.5 SUBTASK 1.5 – PERFORM AND MAINTAIN PROGRAM QUALITY CONTROL (QC)**

The contractor shall ensure that a high quality of service is maintained throughout the life of this TO. The contractor shall employ realistic and substantial methods and monitoring techniques for improving the overall quality of the CDM Technical Support Services. The contractor shall update the QCP periodically to include the following:

1. The contractor's overall approach and procedures for communicating with the Government, resolving deficiencies, and identifying potential improvements;
2. A description of the contractor's internal review process to include who will perform the review, the frequency, the method and a listing of services/products/capabilities under review;
3. The benchmark metrics and measures that will be used to evaluate internal program performance and identify improvement areas and the process for achieving the performance objectives;
4. The contractor's approach and procedures for handling corrective action, without dependence upon Government direction, and for implementing potential improvements to program services/products/capabilities.

##### **4.1.5.1 UPDATE QUALITY CONTROL PLAN (QCP)**

The contractor shall update the QCP submitted with their quote **(Deliverable 10)** periodically as changes in program processes are identified, or annually if no changes are identified.

#### **4.1.6 SUBTASK 1.6 – CONDUCT TRANSITION**

A transition shall ensure minimum disruption to vital Government business. The contractor shall ensure that there will be no service degradation during and after transition. The contractor shall propose and implement a Transition-in and out Plan for the migration of current operations.

##### **4.1.6.1 PERFORM TRANSITION IN**

The contractor shall execute their transition in approach to ensure minimum disruption to vital Government business. The contractor shall ensure that there will be no service degradation during and after transition. The contractor shall implement their Transition In Plan to facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the award of the TO. The plan shall identify and discuss the existing roles and responsibilities of the incumbent contractor and information expected from the incumbent. The plan shall also identify the roles and responsibilities of the contractor, transition of the CDM PMO support including proposed schedule(s), milestones, and deliverables. The contractor shall identify any actions contemplated on the part of the Government. The Transition-In Plan shall be provided as part of the contractor's quote submission.



#### **4.1.6.2 PERFORM TRANSITION OUT**

The contractor shall implement the Transition Out Plan that has been provided NLT ninety (90) days prior to expiration of the TO (**Deliverable 11**). The Transition-Out plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor /Government personnel at the expiration of the TO. The contractor shall identify how it will coordinate with the incoming and or Government personnel to transfer knowledge regarding the following:

- Project management processes
- Points of contact (POC)
- Location of technical and project management documentation
- Status of ongoing technical initiatives and training events
- Appropriate contractor to contractor coordination to ensure a seamless transition.
- Transition of key personnel
- Identify schedules and milestones
- Identify actions contemplated on the part of the Government.
- Establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings.

#### **4.1.7 SUBTASK 1.7 – PROVIDE FINANCIAL REPORTING**

The contractor shall provide a Financial Report of cumulative expenditures monthly (**Deliverable 12**) to the COR. The Financial Report shall include as a minimum the following:

1. Project monthly expenditures and labor hours by CLIN and TO level starting with the current month through the end of the POP.
2. Funded levels by CLIN
- 3 Labor hours incurred to date by CLIN
4. Diagram reflecting funding and burn rate by month
5. Cumulative invoiced amounts for each CLIN up to the previous month.
6. Actual current and cumulative dollars expended for small businesses compared to TO subcontracting goals.
7. Invoice back-up and supporting documentation.

The contractor shall present a Financial Report format at the Project Kick-Off Meeting for Government review. The Government will provide written approval of the proposed format via the COR, and this approved format shall be utilized for the monthly financial reporting requirement. The Government may request updates to the format based on DHS CDM PMO requirements.

## **4.2 TASK 2 – PROVIDE ENGINEERING SUPPORT**

The contractor shall support the CDM Engineering Team by providing technical expertise and support to develop requirements and ensure compliance. Support includes providing technical input and insight related to DEFEND and the Dashboard efforts, review of RFSs, future capability and requirements definition, review of SELC deliverables and review project change requests to provide technical scope recommendations.

### **4.2.1 SUBTASK 2.1 PROVIDE CDM PORTFOLIO TEAM ENGINEERING SUPPORT**

The contractor shall provide engineering support to assist the government and each DEFEND Portfolio (DEFEND A-F (DEFEND F is anticipated to be awarded in FY20. Prior to that the contractor shall support Task Order 2F) and Dashboard portfolio team). Engineering support includes providing analysis of requirements and design specifications, oversight of ongoing CDM DEFEND engineering activities and recommendations to fix the problems with various solutions. Each portfolio team consists of a Government Leads including a CDM Portfolio Manager, Engineer, Acquisition lead and Test POC, who specifically support a portfolio of agencies overseeing their deployment and integrations of CDM capabilities. The contractor shall support each portfolio team by providing additional IA and cyber engineer subject matter expertise. The DEFEND portfolio teams participate in approximately 24-30 meetings per week. Weekly meetings vary and are internal, with agencies, and DEFEND integrators. The contractor shall participate in the meetings as required; assist the engineer in documenting the technical discussion, follow-up on engineering activities, and track status. The contractor shall support the Government with engineering activities to include, but not be limited to the following:

1. Review technical deliverables from ongoing CDM DEFEND and Dashboard activities
2. Support the DEFEND portfolio team in the development, drafting, review and/or QA of technical aspects for current and future RFSs. The contractor shall also participate in the review of RFS Technical Deliverables, responses and ROMs perform technical analysis and recommendations to the Government. The contractor shall assist the Government in overseeing the technical planning and implementation of RFSs, tracking and reporting progress and issues.
3. Participate and perform technical and capability analyses required for approved projects to include, but not limited to data quality tiger teams, storage solution Dashboard reviews, Logical Data Model reviews, Big Data Storage Solutions and other focus groups, etc.
4. Support design specifications for project specific requirements and assist with the planning and execution for the implementations into detailed Phases in-line-with CDM program objectives.

5. Assist with the development of specific implementation designs and enhancements for CDM PMO partner organizations (Agencies, NCCOE, NCCIC, etc.) based on program objectives and feedback.
6. Assist with review of test plans, test execution and test results evaluation.
7. Provide relevant technical input to the Life Cycle Cost Estimate (LCCE) through cross product team engagements. The contractor shall also provide engineering expertise to assist in the development of RFS IGCEs.
8. Assist in the review and validation of the following programmatic artifacts to include, but not limited to the following
  - a. SELC Planning Artifacts (CONOPS, etc.)
  - b. Functional Requirements and Capabilities Documentation
  - c. DEFEND TO Deliverables
    - Integrated Master Schedules (IMSSs)
    - Implementation and Back-out Plans
    - Solution Implementation Architecture (SIA)
    - System Design Documentation
    - Plan for Transition to Agency Production Operations
    - Requirements Traceability Matrices (RTMs)
  - d. RFS packages and deliverables
  - e. LCCE updates
  - f. Risk Register Inputs
  - g. Project Plans

The contractor shall support the CDM DEFEND and Dashboard Portfolio Team by reviewing the above documents, providing comments, and participating in red team reviews.

#### **4.2.2 SUBTASK 2.2 – PROVIDE CDM CAPABILITY SUBJECT MATTER EXPERTISE**

The contractor shall provide subject matter expertise to assist the government with providing specialized technical input on specific CDM capabilities and tools. The contractor shall provide specialized technical subject matter expertise to support the technical application of existing and future CDM tools, analysis of requirements and design specifications, development of CDM capability requirements, and provide consultation and recommendations to on various solutions. In addition to supporting the full set of capabilities listed in Section 3.3, the CDM PMO has a

focused need for cyber capability subject matter experts in Cloud, Mobile, Identity and Access Management, Data Protection, Network Defense, Digital Forensics/Incident Response, and Risk Compliance. The need may grow to include supplemental support to the above capabilities or future capabilities. The contractor shall provide specialized SME on the CDM PMO focused capabilities on an on-going basis, as well as support to all of the capabilities in Section 3.3 on an as needed basis. The contractor shall provide subject matter expertise to include, but not be limited to, the following activities:

1. Support the ongoing refinement of Network Security Management and Data Protection requirements listed in section 3.3, as well as any future capabilities.
2. Assist the Government in the review and generation of documentation with respect to project specific operational concepts
3. Engineering cybersecurity solution subject matter expertise:
4. The contractor shall provide SME on CDM products and tools that are currently deployed and planned to be deployed at the agencies. Some current CDM products examples include RSA Archer, Splunk Enterprise and SailPoint IdentityIQ. Future products may be Mobile Device Management Products, Data Protection Products, Network Boundary Protection Products, etc. The contractor shall familiarize themselves with the CDM Approved Products List (APL) located at the following: (<https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm-program>) which contains all of the products of interest to CDM PMO.
5. Reachback SME to Portfolio Teams on specific capabilities and tools in support of deployment activities to include monitoring specific capability activities and document reviews to ensure technical solutions meet RFS requirements. The contractor shall adequately review and provide analysis and recommendations on technical solutions, Analysis of Alternatives (AoAs) and Technical change requests.
6. Evaluate technical trends and provide recommendations for technology and architecture to meet the CDM program objectives for the government review and acceptance.
7. Identify and/or recommend products, tools or technologies which will expand the CDM capability base, in particular, for Data Protection and any future capabilities.
8. As necessary, interface with agency stakeholders to provide focused support and artifact development to produce comprehensive and effective RFSs
9. Support CDM Program future capabilities and address changes in technology
10. Assist the CDM Capability Development Team (CDT) by providing input and drafting of CDM capability requirements and any supporting documentation.
11. Assist in the validation of the following programmatic artifacts to include, but not limited to the following:
  - SELC Planning Artifacts (CONOPS)

- Functional Requirements and Capabilities Documentation
- RFS packages and deliverables
- LCCE updates
- Risk Register Inputs
- Project Plans

#### **4.2.3 SUBTASK 2.3 PROVIDE CDM PROGRAM STRATEGIC AND TECHNICAL PLANNING (OPTIONAL)**

The CDM program architecture is ever evolving and must remain nimble to keep pace with the changing cyber threat. The contractor shall provide support to the architecture planning efforts as well as supporting the government with assessments of objectives and conducting gap analysis of existing versus required capabilities. The contractor shall provide CDM Program Strategic and Technical Planning support to include, but not be limited to, the following activities:

1. Assist the government by conducting evaluations of requirements to identify potential software, hardware, and system architectures that can be employed.
2. Plan, develop, assess and validate requirements, specifications, hardware and software selections, including commercial off-the-shelf (COTS)
3. Refine and identify CDM current and future capabilities and requirements
4. Technical support for the development of reference network architecture supporting CDM within legacy on-premise, cloud, and hybrid Agency networks.
5. Assist the government with development of potential technical solutions to support AoAs for best-fit solutions.
6. As applicable, evaluate technical trends and provide architecture recommendations to assist the CDM PMO in meeting the CDM program objectives.
7. Assist the government in the drafting, coordinating and/or maintaining program capabilities, requirements and technical documentation.
8. Assist the contractor in the development of data models, CDM Master Record data, concepts of operations and requirements that support new and existing architectures.
9. Validate and support implementations to include, but not limited to the following:
  - Review and validate implementation approaches and strategies.
  - Monitor implementations to ensure solutions conform to target architecture
10. Assist the government by providing program level architecture support to the CDM PMO. Support includes attending external meetings in order to capture feedback and recommendations on current and future capabilities and requirements
11. Support CDM PMO in working with partner organizations, DHS components, and other Federal Agencies in the communication and development of CDM concepts and architectures.

12. Subject matter expertise, review and validation on the following programmatic artifacts to include, but not limited to the following:

- Architecture and Capability artifacts
- Technology insertion
- RFS packages and deliverables
- LCCE updates.

#### **4.2.4 SUBTASK 2.4 PROVIDE RESEARCH AND DATA MODELING TECHNICAL SUPPORT (OPTIONAL)**

The CDM PMO fully expects the data generated by Agencies reporting to the Dashboards to increase exponentially in the very near future. This data landscape offers a unique opportunity to develop and mature new models and metrics for identifying and measuring cyber risks. The contractor shall provide the following research and technical analysis support to include and not limited to the following:

- Provide research and technical analysis expertise for CDM Data Metrics support to develop government wide cybersecurity metrics, covering statistical data gathering methods, data analysis correlation/aggregation algorithms, and dashboard reporting
- Conduct research to identify potential opportunities to apply mathematical and/or statistical analysis in order to frame cyber risk measurement problems and build risk models and indices based on Federal Agency data
- Support CDM data modeling and data management activities.

### **4.3 TASK 3 – SUPPORT CDM PROGRAM DASHBOARD OPERATIONS**

The CDM Dashboard is the critical measure of the CDM PMO success. It serves as the operational depiction of Federal and Agency IT environments and provides actionable information for agencies to address issues across their respective enterprise. The current CDM dashboards supports the following:

- Receipt, collection and development of situational awareness visualization of data on network assets, user accounts and other network activities from the Agency-level Dashboards to the Federal Dashboard
- Measurement of cyber relevant datasets, including misconfigurations and vulnerabilities
- Reporting results to Federal officials through a web-based user interface with organizationally defined reports and ad hoc querying.

The CDM PMO has an existing Task Order for the development of the Dashboard, which requires the contractor to deliver iterative releases of the Federal and Agency CDM Dashboard (approximately two to three per year).

The CDM PMO requires contractor support to assist the Government with general operations support and oversight of the Dashboard releases, to include internal management, tracking and reporting of Dashboard releases.

#### **4.3.1 SUBTASK 3.1 – SUPPORT RELEASE MANAGEMENT ACTIVITIES**

The Government desires a unified view of the various DEFEND and Dashboard workstreams to assist the CDM PMO in streamlining efforts, reduce the burden on reporting of status and to enable better release management activities of CDM Dashboard (both Agency and Federal) and the data integration activities supporting the CDM Solution across Group A-F. Data integration may include, but is not limited to; custom code development for connectors/skims for tools/sensors, python/java/C#/javascript, APIs and documentation and/or validation of the CDM integrators approach, design and implementation of the Master Device Record (MDR), Master User Record (MUR), Master Incident Record (MIR), Master System Record (MSR).

Release management is the process of managing, planning, scheduling and controlling a software build through different stages and environments; including testing and deploying software releases. The Engineering SME service contractor shall use best practices in developing a release management methodology for the safe, effective, orderly and successful release and management of each version of the CDM Solution and CDM Dashboard to include, but not limited to performing the following activities:

1. For entire CDM Solution and Dashboard, participate in the development of and maintain a CDM Product Roadmap (**Deliverable 13**) that strategically aligns to the CDM program's goals for integration of the high-level capability themes (e.g. Manage Assets, Manage Identities and Access, Manage Network Events, and Data Protection, Agency and Federal Dashboard).
2. For CDM Dashboard, collaborate in requirements sessions of the CDM Dashboard to facilitate Release Management:
  - Facilitate the identification of a prioritized list of features for each release of the dashboard based on:
    - the strategic goals of CDM program,
    - technical capabilities of the core dashboard solution (and/or its various modules)
    - CDM stakeholder defined needs, input and
    - targeted implementation timeline (schedule) for a sub-set capabilities (e.g. Risk Scoring (AWARE), Ongoing Assessment, Incident Response) as aligned to the program's roadmap. Examples include, but not limited to; feature alignment with most current version of CDM Logical Data Model, implementation of a sub-set of capabilities Network Access Control (NAC), etc.

- Provide technical and managerial input to facilitate a prioritized list of features for each release (**Deliverable 14**) of the CDM Dashboard for Government approval. Communicate the prioritized list of features with appropriate stakeholders (e.g. Dashboard Provider).
- 3. For entire CDM Solution, collaborate with DEFEND Integrator for all custom code developed to support data integration activities across Group A-F. Data integration includes, but is NOT limited to; development of custom code connectors/skims for tools/sensors, python scripts, APIs and documentation and/or validation of the CDM integrators approach, design and implementation of the Master Device Record (MDR), Master User Record (MUR), Master Incident Record (MIR), Master System Record (MSR).
  - Manage custom code from DEFEND integrator in a repository (e.g source code and/or releasable compiled code as applicable).
  - Manage, review artifacts (e.g. Requirements Documentation, Sprint Planning Documents, Retrospective Documents and gap requirements, and updated/refined user stories), coordinate communication activities, and store metric reports. Develop after action release reports.
- 4. For entire CDM Dashboard, collaborate with Dashboard Provider to facilitate Release Management for each release of CDM Dashboard (both Agency and Federal) and collaborate with Dashboard Provider for all custom code developed that includes, but is NOT limited to;.NET, C#, Python, Java, Javascript, API's).
  - Manage dashboard release packages in a repository (e.g source code and releasable compiled code for both Agency and Federal Dashboard).
  - Manage, review artifacts (e.g. Requirements Documentation, Sprint Planning Documents, Retrospective Documents and gap requirements, and updated/refined user stories), coordinate communication activities, and store metric reports. Develop after action release reports.
- 5. For CDM solution(s) and CDM Dashboard, lead and collaborate with DEFEND Integrator and Dashboard Provider to provide Test Case Management of each release.
  - Manage, review artifacts for pre-release verification and validation of functionality aligned with CDM SELC Tailoring Plan. Artifacts may include, but are not limited to manual and/or automated test cases, coverage of test scripts and User Acceptance Tests (UAT) with an agency, with the Government providing Independent Verification and Validation (IV&V).
  - Manage, review artifacts for post release validation and possible roll back of each implementation of the CDM Dashboard aligned with CDM SELC Tailoring Plan. Artifacts may include, but are not limited to integration smoke tests, Post Implementation Review to assess the impact of the current release deployed to all agencies and the Federal level.
  - Coordinate communication activities, and store metric reports.



- Develop after action release reports.
  - Manage and review artifacts (e.g. manual and/or automated test cases, coverage of test scripts), coordinate communication activities, and store metric reports.  
Develop after action release reports.
6. Automate the execution of this task using tools and custom workflows, such as Atlassian JIRA and Confluence, which is currently available on the DHS ALMSS platform or recommend other such tools as necessary. Have experience with tools that add productivity to oversight and management activities, examples include, but are not limited to the following:
- JIRA: Issue and project tracking for traditional and agile projects.
  - Confluence: Per-project, collaborative document editing.
  - CloudBees: Automated software build, test, integration, and performance profiling.
  - Artifactory: Stores software artifacts and resolves dependencies for maven builds.
  - Gitlab Source Control: Distributed, efficient source control and versioning.
  - SonarQube, Selenium, OWASP ZAP – Code Reviews: Manage code quality and perform code reviews.
  - Twistlock – full-lifecycle container and cloud native cyber security.
  - Storefront – Reusable Components: A registry of reusable applications, services and components (python scripts, connectors, etc).
  - Secure File Sender: Makes it easy to securely transfer large files using only a web browser. Files can be transferred to one or several recipients.
  - IBM Rational DOORS: Requirements Management software
  - ServiceNOW: Incident and IT service management software
  - Microsoft Sharepoint: Team Collaboration software with document management capabilities
  - Microsoft Team Foundation Server: Development management tool (source code, requirements management, project/release management)
  - Microsoft Project (Project Server): Project Management software

#### **4.3.2 SUBTASK 3.2 – PERFORM DASHBOARD OPERATIONS AND MAINTENANCE**

The contractor shall perform the following dashboard operations and maintenance to include, but not limited to the following:

1. Perform activities necessary for Certification and Accreditation (C&A) of Federal Dashboard and coordinate with Dashboard contractor and ISSO.
2. Manage and create processes for creation, distribution, and tracking of PKI certificates.
3. Manage, track and report user accounts for Federal Dashboard.
4. Manage and track change control documents submitted to DHS Sustainment. Changes include things like Port Open Requests, Server upgrades, infrastructure upgrades, etc.
5. Review engineering change documents and contract document deliverables and make recommendations to the CDM PMO portfolio teams and/or leadership

#### **4.4 TASK 4 – ASSESS AGENCY READINESS AND PROVIDE RFS SUPPORT**

To achieve program success, the CDM PMO must work with the Agencies to align and sequence the development and implementation of CDM capabilities with Agency requirements. In concert with awarding the DEFEND Task Orders, the government established a flexible approach to meeting the ever evolving CDM capabilities as well as individual agency requirements. The RFS process is the mechanism that will address both CDM PMO and Agency-specific requirements for delivery and/or additional support of a CDM capability or service.

Understanding the absorptive capacity of the various agencies is paramount to efficient roll-out and execution of CDM capabilities through the RFSs process. The contractor shall provide SME to assist the CDM PMO in assessing Agency CDM capabilities, needs and create a deployment plan of executing CDM capabilities based on the readiness of the Agency. This assessment should detail the environment for each organization and identify an Agency's ability to absorb and implement Network Security Management and Data Protection foundational capabilities and any future capabilities as identified in section 2. Assessment activities shall be from document reviews or in-person interviews with contractors, or government personnel to determine if an Agency has the ability to deploy a CDM capability solution and a schedule for when the solution could be deployed. This task creates a roadmap for each agency to deploy CDM capabilities over the life of the DEFEND Task Order and beyond.

Additionally, the contractor shall provide support to each of the portfolio teams in the development, management, and oversight of the Capability Management process.

##### **4.4.1 SUBTASK 4.1 – ASSESS THE AGENCY ENVIRONMENT (OPTIONAL)**

Over the last few years, the CDM PMO has worked to mature and sequence program capabilities and requirements across a dynamic Federal landscape. Despite significant synchronization efforts and concerted planning, there may be instances where participating CDM Agencies do not have the absorptive capacity to receive a particular CDM capability or that an Agency may have priorities that do not align with a particular CDM capability. The CDM PMO needs to understand these Agency gaps to better synchronize and sequence our CDM capability roadmap.

#### **4.4.1.1 SUBTASK 4.1.1 – ASSESS THE AGENCY ENVIRONMENT FOR RECEIVING NETWORK SECURITY MANAGEMENT CAPABILITIES (OPTIONAL)**

As required, the contractor shall provide an Independent Assessment Report (**Deliverable 15**) for each Agency detailing the Agency's environments and the readiness to implement Phase 3 CDM tools and capabilities as identified in Section C.4.3.1. The Independent Assessment Report will assist both the CDM PMO and the agency in developing a capability roadmap to identify and execute CDM capabilities through the RFS process. The Independent Assessment Report shall include, but not limited to the following:

1. Draft surveys, questionnaires, checklists, and any assessment documents used.
2. Identification of shortfalls including key factors/drivers.
  - a. Assessment of potential options
  - b. Preferred plan with key milestones, a schedule, and prerequisites for agency preparedness for execution
  - c. An independent cost estimate to deploy a CDM Capability across an entire Agency. The independent cost estimate shall include costs such as labor, overhead, materials, equipment, travel, etc.
3. Documents gathered from the assessment that will aid in planning for Agency support of provisioning, configuring, operating, testing, and managing CDM tools, sensors, Agency-level dashboards, and data feeds as well as support for CDM Solution's governance.
4. A prioritized list of the capabilities the Agency wants to deploy, and when they would be ready to deploy them based on Agency input and independent analysis.
5. Identification of any training required.
6. An assessment on the maturity in relation to receiving a new CDM capability or an enhancement of a CDM capability. Considerations for Policy, Governance, Infrastructure, etc. should be included in this assessment.
7. An independent assessment of existing and planned CDM capabilities and the probability of success in deploying enhancements or capabilities.

#### **4.4.1.2 SUBTASK 4.1.2 – ASSESS THE AGENCY ENVIRONMENT FOR RECEIVING DATA PROTECTION CAPABILITIES (OPTIONAL)**

The contractor shall provide an Independent Assessment Report (**Deliverable 15**) for each Agency detailing the Agency's environments, validating Agency High Value Assets (HVAs) number and structure, and determining the readiness to implement Data Protection CDM tools and capabilities as identified in Section C.4.3. The Independent Assessment Report will assist both the CDM PMO and the agency in developing a capability roadmap to identify and execute CDM capabilities through the RFS process. The Independent Assessment Report shall include, but not limited to the following:

1. Draft surveys, questionnaires, checklists, and any assessment documents used.
2. Identification of shortfalls including key factors/drivers.
  - a. Assessment of potential options
  - b. Preferred plan with key milestones, a schedule, and prerequisites for agency preparedness for execution

- c. An independent cost estimate to deploy a CDM Capability across an entire Agency. The independent cost estimate shall include costs such as labor, overhead, materials, equipment, travel, etc.
3. Documents gathered from the assessment that will aid in planning for Agency support of provisioning, configuring, operating, testing, and managing CDM tools, sensors, Agency-level dashboards, and data feeds as well as support for CDM Solution's governance.
4. A prioritized list of the capabilities the Agency wants to deploy, and when they would be ready to deploy them based on Agency input and independent analysis.
5. Identification of any training required.
6. An assessment on the maturity in relation to receiving a new CDM capability or an enhancement of a CDM capability. Considerations for Policy, Governance, Infrastructure, etc. should be included in this assessment.
7. An independent assessment of existing and planned CDM capabilities and the probability of success in deploying enhancements or capabilities.

#### **4.4.1.3 SUBTASK 4.1.3 – PERFORM FUTURE CAPABILITY ASSESSMENTS (OPTIONAL)**

CDM capabilities evolve rapidly to keep pace with threats, market leading tools and agency priorities. The CDM PMO must maintain a synchronized roadmap with Federal Agencies. Thus, as the CDM PMO identifies new capabilities and requirements, the contractor shall conduct an assessment similar to Sections 4.4.1.1 and 4.4.1.2 or as defined/tailored by the CDM PMO.

#### **4.4.2 SUBTASK 4.2 – PROVIDE RFS SUPPORT**

An RFS is essentially a requirements package that is developed by the CDM PMO or Agency and provided to the DEFEND Integrators for response and execution (see Section 3.5). The CDM PMO has chartered a RFS working group to synchronize RFS development activities and manage and track the sequencing of RFS roll-outs.

The contractor shall provide direct support to the CDM RFS Working Group in order to manage, develop and track CDM PMO and Agency RFSs to include, but not limited to the following:

1. Develop, refine and review requirements needs statements within the RFS document
2. Develop and review cost and/or resource estimates in support of the RFS package
3. Assist the government in the management and administration of RFS and resource priorities throughout the RFS process
4. Track the development and execution of RFS for all DEFEND orders.
5. Support the acquisition team and DEFEND technical points of contact (TPOCs) in the management of RFS artifacts and deliverables.

#### **4.5 TASK 5 –PROVIDE REQUIREMENTS DEVELOPMENT AND MANAGEMENT SUPPORT**

The contractor shall support the program lifecycle team in formulating and managing CDM program requirements. Specifically, the contractor will be required to assist the government in managing the development of CDM capabilities through open source tools, developing and/or refining program acquisition documentation, provide research and technical editing for CDM requirements documentation as well as configuration management support as necessary.

##### **4.5.1 SUBTASK 5.1 PROVIDE CDM AUTOMATED SOLUTIONS**

The management of the various active CDM development task orders as well as capabilities development activities will create a massive information and process management requirement. The sheer number of potential CDM capabilities, requirements, change requests, program or project risks and other programmatic information will be challenging to manage and track manually, even with market leading tools and streamlined processes. Where possible, the government needs processes and tracking mechanisms automated. The contractor shall work to develop automated processes to allow the PMO to efficiently manage the vast number of contract and programmatic requirements. .

##### **4.5.1.1 SUBTASK 5.1.1 – PROVIDE ALMSS ATLIASSIAN TOOL SUPPORT AND TRAINING**

The contractor shall provide highly-specialized support to configure and maintain a CDM PMO project space within a DHS enterprise-provided solution via the Atlassian tool suite. Access to the Atlassian Application Lifecycle Management Software Suite (ALMSS) is provided at no cost to any DHS component by the DHS Office of Chief Information Office (OCIO). At its core, Atlassian is a suite of applications composed of various products which integrate with each other. The CDM PMO plans to utilize JIRA, Confluence, and JIRA Service Desk and other ALMSS tools as platforms to help manage the flow of work, enhance communication and tracking of needs, and support stakeholders through use of a ticket-based system. All of these elements are highly customizable and integrate with each other to link work across the organization. Work within the Atlassian suite can be organized by project, allowing the CDM PMO to track issues at a project level with complete transparency using granular user permissions or by team through using Agile principles and Kanban boards to visualize work. The contractors shall provide tailored instances of the Atlassian platform and domain expertise to train users allowing for the reduction of waste and duplicative efforts. Currently, ALMSS is being utilized as an automated tool to support the CDM Program requirements adjudication process. ALMSS captures and tracks stakeholder (internal DHS (FNR/NCCIC, etc.), Agencies, System Integrators and others needs and CDM requirements.

The contractor shall provide continuous customization, tracking, administration and health analysis for the CDM Program requirements adjudication process and all requested ALMSS projects. The contractor shall provide support to include, but not limited to the following:

1. Tailor ALMSS tools to provide a unified dashboard that enables CDM PMO leadership to clearly digest the health of projects (i.e. project risks, efficiency, scope, milestones and scheduling)
2. Provide ongoing customization support to meet the unique requirements of each project
3. Provide the ability to track and score potential projects as a method for identifying needs for additional contractor support (i.e. Agile coaching, Technical domain experts etc.)
4. Allow for the scoring and rating of new and existing projects enabling an CDM leadership to rank and approve projects for implementation
5. Provide initial ALMSS training, develop, update and maintain user guides, ad hoc support and continuous training to ensure the CDM PMO users understand the maximum utilization of ALMSS and its full potential
6. Provide research and recommendations on either a Manual or Automated process for integration/and or exchanging of Data between the ALMSS Tools and Dynamic Object Oriented Requirements (DOORS).

#### **4.5.1.2 SUBTASK 5.1.2 – PROVIDE CAPABILITIES DEVELOPMENT MANAGEMENT**

Almost all CFO Act Federal Agencies and a host of smaller agencies have participated in the CDM program through previous Task Orders and have implemented CDM solutions. As the CDM PMO continues to refine and roll-out capabilities, the ability to manage and track present and future implementations becomes challenging. Additionally, the CDM PMO's internal and external programmatic reporting capabilities must also increase as Federal oversight increases.

The CDM PMO requires assistance in managing capabilities development and implementation activities. The contractor shall provide capabilities development and implementation support to include, but is not limited to the following activities:

7. Identify or develop a tool (open source) to automate, track CDM capabilities, CDM capabilities development activities, implementations and deployments across all DEFEND Agencies and components to completion.
8. Assist the government in developing and gathering capability programmatic metrics ranging from costs to requirements closure tracking.
9. Assist in the management and reporting of program capabilities to include briefings or depictions that may serve as formal external communications
10. Administer, train and provide operations support to the PMO's requirements tools and processes
11. Assist the government in defining and ensuring consistency and traceability of all requirements, including interface requirements

#### **4.5.1.3 SUBTASK 5.1.3 – PROVIDE ENTERPRISE WIDE AUTOMATED SOLUTIONS (OPTIONAL)**

The contractor shall develop a tool or solution which automates and/or links all the internal program review boards, processes, workflows and trackers. The contractor shall review and

assess all CDM existing processes and workflows and recommend a knowledge management solution to better automate and link. The CDM PMO currently utilizes tools such as SharePoint and Excel to manage and track things like Configuration Control Board (CCB) requests, Program and Project Risk, RFSS, CDM APL, CDM Tool and License Management, CDM Deliverables, Project Work book, etc. The contractor shall review all existing processes, recommend, design, implement and administer an automated and/or enterprise wide solution based on Government review and approval. Based on the contractor's review they shall also identify and recommend any new processes to be automated. Additionally, the contractor shall develop a CDM PMO reporting dashboard that can be viewed by internal and external stakeholders in real time displaying enterprise summary data from the various management tools and processes.

#### **4.5.2 SUBTASK 5.2 – PROGRAM MANAGEMENT ACQUISITION AND ORGANIZATIONAL SUPPORT**

The PMO has established various boards, systems and processes to drive project and program decisions. While the portfolio teams are largely responsible for work leading up to a particular decision board or process, the CDM PMO requires support to assist with the management and administration of IPT activities associated with the decision making process. Additionally, as the CDM Program grows exponentially, the acquisition and programmatic reporting requirements increase. The contractor shall provide direct support to the CDM PMO acquisition, risk and requirements management and lifecycle support teams. The contractor shall provide the following support to include, but are not limited to the following:

1. Support the CDM PMO Risk IPT;
  - Identify, analyze, and capture risks for the CDM PMO. The contractor shall maintain the risk registry and updates, identify and categorize risks, and coordinate with other Government IPTs and external partners/organizations.
2. Support the CDM PMO Requirements Management Board (RMB) and process to include facilitation, administration, workflow and documentation reviews.
3. Support the government with creation of program level acquisition documentation and briefing materials for the CDM PMO.
4. Provide acquisition and programmatic expertise in support of CDM PMO acquisition baseline reviews.
5. Assess the probability and potential impact to the technical, cost, schedule, management, and other program objectives.
6. Provide relevant technical input to the LCCE and retain ongoing traceability to requirements and programmatic updates.
7. Facilitation and administrative support to the PMO configuration change board (CCB).
8. SME and validation support to the following programmatic artifacts to include, but not limited to the following):
  - Functional Requirements and Capabilities Documentation

- LCCE updates
- Acquisition Review Board inputs
- Risk Management Tracking tools.

#### **4.5.3 SUBTASK 5.3 – PROVIDE TECHNICAL WRITING SUPPORT**

As the CDM program further defines and refines its capabilities, the PMO requires assistance in capturing, distilling and communicating information to both internal and external stakeholders. The contractor shall provide technical editing and writing expertise to various teams within the CDM PMO. While the support will be focused on the engineering and program lifecycle activities, the contractor should keep abreast and possess an understanding of the many facets of the program. The contractor shall provide the following support to include, but not limited to the following activities:

1. Technical writing expertise in support of Tasks 2, Task 5 and Task 6 activities and documents.
2. Gather, translate and compose technical information into clear, readable documents for use by both technical and non-technical personnel.
3. Support the CDM PMO capability development teams (CDT) in drafting CDM capabilities and technical supporting documentation.
4. Support RFS WG in writing and editing RFSs. The contractor shall review and technically edit documents.
5. Support the review and/or edits of agency submitted RFS
6. Support the government with creation of technical materials for the CDM program
7. Update and develop documents that support the DHS System Engineering Lifecycle to include, but are not limited to Concept of Operations, Operational Requirements Document, System Requirements, System Design, Test & Evaluation Management Plan
8. Perform document editorial review and updates.

#### **4.6 TASK 6 – PROVIDE TEST AND EVALUATION SUPPORT**

At present, all CDM Task Orders and RFSs associated with the CDM solution are expected to follow a tailored approach when conducting engineering and testing activities. As previously described, the SELC describes that process for the implementation and integration of CDM solutions. The contractor shall support the full spectrum of testing activities to ensure the DEFEND and Dashboard solutions satisfy mission requirements IAW the associated SELC Phases. This includes the contractor providing test function SME support, where these functions are allocated across projects and programs as needed and/or requested.

While the contractor provides direct CDM PMO support, the PMO may use other independent contractors or FFRDCs to provide assessments, develop or review testing artifacts, and/or



oversee developmental, functional, integration and operational testing. The contractor shall work in concert with the independent testing entities to ensure alignment with programmatic objectives.

#### **4.6.1 SUBTASK 6.1 – PROVIDE CDM PMO TEST TEAM AND DEFEND PORTFOLIO SUPPORT**

The contractor shall support the government CDM PMO test team and the DEFEND and Dashboard portfolio groups. While the government does not require individual support for each DEFEND group, the contractor should expect to be embedded with the CDM PMO test team and utilized to support DEFEND and Dashboard test activities; develop, refine and review Task Order deliverables; and provide broader CDM requirements support.

The contractor shall provide the following support to the CDM Test Team include, , but not be limited to the following activities:

1. Support various program and TO T&E IPT or working groups
2. Validate DEFEND TO Test related documentation and activities to include:
  - TEMP
  - Level 1 testing
  - Level 3 testing
  - User Acceptance Testing
  - Development of Test cases and plans
3. Work with DEFEND portfolio teams, integrators and end users to plan and prepare for all testing activities
4. Provide support to technical meetings, working groups, and technical reviews during test execution
5. Validate specific DEFEND Requirements Traceability Matrices to ensure compliance with CDM Program Test plans
6. Assist in coordination of testing activities with CDM PMO, FFRDCs and other Test Authority Organizations

#### **4.6.2 SUBTASK 6.2 – PROVIDE PROGRAMMATIC TEST AND EVALUATION SUPPORT**

The contractor shall play an important role in helping the government develop Program-level requirements and test documentation as well as maintain traceability between functional and system level documentation. The contractor shall provide support to include, but not limited to the following

1. Update Major Testing Program Documentation updates on an annual basis (or as required by activity).

2. Support to Operational Test and Evaluation (OT&E) certification activities by reviewing test result briefings, certification recommendations, and other necessary documentation to demonstrate that OT&E risks have been sufficiently mitigated.
3. Provide test support to the CDM Requirements Management Board (RMB) for major program documentation updates and development of program documentation.
4. As required provide support the development and maintenance of the program level RTM.

#### **4.7 TASK 7 – PERFORM CDM TOOL MANAGEMENT**

The CDM Solution maintains a degree of consistency across the Group C Agencies by leveraging a similar set of Commercial Off-the-Shelf (COTS) tools. These tools have been reviewed by the DHS CDM PMO to identify that they meet the capabilities of, or in conjunction meet, the requirements specified in CDM Technical Capabilities Requirements Document, Volumes 1 and 2. The contractor shall support the PMO in the management of the tool approval process as well as the tracking and management of CDM tool procurements.

##### **4.7.1 SUBTASK 7.1 PERFORM APPROVED PRODUCTS LIST ADMINISTRATION AND MANAGEMENT**

The CDM program office maintains a list of approved products that supports the various CDM solutions. The CDM PMO charters a technical evaluation team which reviews vendor submissions of products for inclusion on the APL. The contractor shall support the monthly evaluation of new product submissions for consideration to be added to the APL. The contractor shall provide the following support to include, but not limited to the following:

1. Conduct conformance checks to assure that the product submission are within CDM PMO process standards.
2. Update, track and manage submissions to ensure high fidelity data
3. Assemble and file submission documents on SharePoint and communicate with the technical review team when files are ready for Tier 2 review. Upon Tier 2 completion, the contractor shall prepare the package for Tier 3, or DHS Final Technical Review
4. Conduct APL closeout activities, including notifying submitters of their package status, notifying GSA Schedule 70 of product acceptance, and prepare a monthly workbook of what products need to be added, modified, or deleted from the APL.
5. Track, report, query and provide monthly metrics of APL status
6. Manage, update and administer APL and all associated supporting documents to include VPATs, EULAs and SCRM plans.
7. Assist the Government in review, update and enhancements of SCRM plan/questionnaire requirements to better assist an Agency or ordering activity in making a better informed risk decision when considering or using products from the CDM APL.
8. Assist the government in developing and recommending improvements to the data management and automated solutions currently in place

#### **4.7.2 SUBTASK 7.2 – TRACK AND MANAGE CDM TOOLS**

On a daily basis the CDM PMO procures tools and sensors on behalf of Agencies through CDM Task Orders (DEFEND and others). The contractor shall assist the Government in the review, tracking and management of all products procured by the CDM PMO to include, but not limited to the following:

1. Perform quality review of 1149s, DD250s and RIPs for compliance. Identify and notify the Government of any discrepancies.
2. Record and track all CDM tool and sensor procurements in TO workbook and CDM Product master tracker.
3. Review and scrub data on an on-going basis to ensure accuracy and data quality.
4. Query and report on Tool data and pricing by FY, Agency, Phase, manufacturer, etc.,.
5. Recommend tool strategies to meet CDM objectives in maximizing volume discounting.

#### **4.7.3 SUBTASK 7.3– PERFORM TECHNICAL ASSESSMENT OF POTENTIAL PRODUCTS/TOOLS (OPTIONAL)**

The contractor shall assist the Government in conducting technical assessments of tools and sensors submitted for inclusion into the CDM APL. This is a monthly process but can be expedited to meet program needs. The contractor shall provide the following support to include, but is not limited to the following:

1. Verify submitter claims by using data sources that are judged by the Government to be relevant for the product/product families being evaluated.
2. Review submitter and manufacturer websites and independent, unbiased, competent technical evaluation/assessment sources.
3. Assess compliance with CDM Technical Requirements enumerated in the document titled CDM Technical Capabilities Volume Two Requirements Catalog.
4. On a monthly basis recommend and provide feedback to the government on what capabilities the product family meets
5. Identify and recommend to the Government improvements and enhancements to the existing process.

#### **5.0 QUALITY ASSURANCE AND ACCEPTABLE CRITERIA**

The Government will establish and maintain a Quality Assurance Surveillance Plan (QASP) for work accomplished under this contract. The QASP will be based under the following standards and acceptable quality levels (AQL)s:

Std #	PWS Ref	Performance Standard	Acceptable Quality Level
<b>1.</b>	<b>4.0 – 4.7 Tasks 1 -7 and all underlying subtasks</b>	Contractor is reasonable, cooperative, and professional when dealing with other personnel on site, including contractors and Government personnel.	<ul style="list-style-type: none"> <li>No more than two verifiable complaints on a quarterly basis</li> </ul>
<b>2.</b>	<b>4.0 – 4.7 Tasks 1 -7 and all underlying subtasks</b>	Documents are developed, prepared and reviewed in a timely manner with all customer inputs/comments incorporated within.	<ul style="list-style-type: none"> <li>Personnel or workload managers provide acknowledgement of tasking within 2 hours</li> <li>100% of customer inputs/comments are addressed at each phase of the document development.</li> </ul>
<b>2a.</b>	<b>Task 1. (Subtask 1.2)</b>	Management reports (Monthly Status Report (Del. 03), Trip Reports (Del. 04), Meeting Reports (Del 05), Problem Notification Reports (Del. 06)) are developed to include all required information listed in subtask 1.2	<ul style="list-style-type: none"> <li>Per Subtask 1.2, MSR delivered by the 10<sup>th</sup> of each month; Trip Reports delivered w/in 5 days of subject trip; Meeting reports delivered w/in 1 business day after meeting; PNRs delivered 1 business day after problem notified.</li> <li>Management reports are fully compliant with less than 3 substantive errors</li> <li>Substantive and minor errors corrected within 24 hours</li> </ul>
<b>2b.</b>	<b>Task 1 (Subtask 1.3)</b>	In-Progress Reviews (Del. 07) held quarterly	<ul style="list-style-type: none"> <li>Per Subtask 1.3, IPR conducted quarterly</li> <li>IPR presentation materials and any pertinent backups provided to CDM PMO NLT 2 days prior to actual IPR.</li> <li>IPR meeting minutes, to include actions, provided to CDM PMO NLT 5 days after IPR</li> <li>IPR presentation materials have no more than 3 substantive errors.</li> <li>All substantive and clerical errors corrected and submitted with minutes</li> </ul>
<b>2c.</b>	<b>Task 1. (Subtask 1.4)</b>	Project Management Plan submitted to CDM PMO.	<ul style="list-style-type: none"> <li>Initial PMP submitted NLT 30 days after Kick-off meeting</li> <li>Updates to the PMP will happen NLT quarterly but can be updated as necessary</li> <li>PMP will have no more than 3</li> </ul>

			<p>substantive errors</p> <ul style="list-style-type: none"> <li>• All substantive errors will be corrected within 24 hours</li> </ul>
<b>2d.</b>	<b>Task 1 (Subtask 1.6)</b>	Transition-out plan (Del. 11) developed and submitted to the CDM PMO. Transition out plan addresses all aspects of the effort as listed in section 4.1.6.2 of this PWS.	<ul style="list-style-type: none"> <li>• Transition Out plan delivered 90 days prior to end of PoP.</li> <li>• The plan will have no more than 3 substantive errors</li> <li>• All substantive errors will be corrected within 24 hours</li> </ul>
<b>2e.</b>	<b>Task 1 (Subtask 1.7)</b>	Financial Status Report (Del. 12) developed and submitted monthly to CDM PMO	<ul style="list-style-type: none"> <li>• Financial Report provided to CDM PMO on the 10<sup>th</sup> day of Each month as part of the MSR submission.</li> <li>• At a minimum, information listed in list form in section 4.1.7 of this PWS shall be depicted in the report.</li> <li>• The plan will have no more than 3 substantive errors</li> <li>• All substantive and clerical errors will be corrected within 24 hours</li> </ul>
<b>2f.</b>	<b>Task 3 (Subtask 3.1)</b>	CDM Product Roadmap completed and updated in a comprehensive and timely manner	<ul style="list-style-type: none"> <li>• The initial CDM Product Roadmap is developed and delivered NLT 90 days after Contract Kickoff</li> <li>• Updates to the CDM Product Roadmap are comprehensive to include integration efforts for each of the high-level CDM Capability Themes or as depicted by the Dashboard PM</li> <li>• Roadmap updates are provided within the timeline documented by Dashboard PM to align to Dashboard releases.</li> </ul>
<b>2g.</b>	<b>Task 3 (Subtask 3.1)</b>	Dashboard prioritized list of features completed and updated in a comprehensive and timely manner	<ul style="list-style-type: none"> <li>• The initial prioritized list shall be delivered 5 days after the first Dashboard release post-kickoff</li> <li>• Updated features list provided to the Dashboard PM NLT 15 days prior to each scheduled release or the normal quarterly update requirement date</li> <li>• Substantive errors or critical comments are corrected within 3 business days</li> </ul>
<b>3.</b>	<b>Task 2 (Subtask</b>	The Contractor review of the	<ul style="list-style-type: none"> <li>• Comments submitted as part of</li> </ul>

	<b>2.1)</b>	DEFEND TO deliverables are in accordance with DEFEND TO guidelines and guidance of CDM Portfolio Teams	<p>the review of DEFEND TO deliverables will be delivered NLT than the due date prescribed in the DEFEND TO or as designated by the Portfolio Team</p> <ul style="list-style-type: none"> <li>Comments are clear, concise and supportable to ensure the DEFEND Integrator can address issues and reflect updates in the deliverable</li> </ul>
<b>4.</b>	<b>Task 6 (Subtask 6.1 and Subtask 6.2)</b>	Contractor review and validation of RTM and test artifacts (as listed in sections 4.6.1 and 4.6.2) are timely and in accordance with deliverable and DEFEND TO timelines	<ul style="list-style-type: none"> <li>Comments submitted as part of the review of DEFEND TO deliverables will be delivered NLT than the due date prescribed in the DEFEND TO or as designated by the Test Director or CDM Test Team Government Lead</li> <li>Comments are clear, concise and supportable to ensure the DEFEND Integrator can address issues and support testing activities as scheduled.</li> </ul>
<b>5.</b>	<b>Task 7 (Subtask 7.1)</b>	APL metrics report	<ul style="list-style-type: none"> <li>Per Section 4.7.1, Subtask 7.1 contractor monthly report contains less than 3 substantive errors</li> </ul>
<b>6.</b>	<b>Staffing Plan</b>	Maximum Retention of Key Personnel	<ul style="list-style-type: none"> <li>Key Personnel retention as outlined in the staffing plan remained above 66% each year</li> </ul>
<b>7.</b>	<b>Personnel</b>	Minimal gaps in service	<ul style="list-style-type: none"> <li>Contractor replaces all key/non-key personnel in timely fashion. Gaps in Critical resources should not exceed 45 days: Critical resources deemed all key personnel and any other resources that have responsibilities that require interfacing directly with the portfolio teams or CDT or have a technically substantial role in the project's performance.</li> </ul>
<b>8.</b>	<b>4.0 – 4.7 Tasks 1 -7 and all underlying subtasks</b>	Work products are of high quality and are prepared, generated, and delivered with professional care, skill and technical accuracy customary to the profession.	<ul style="list-style-type: none"> <li>No substantive rewrites required except to correct minor clerical errors.</li> </ul>

PROJECT TITLE/LOCATION:

Question No.	RFP Attachment No.	REFERENCE			QUESTION	Government Response
		Page	Section	Para.		
1	Solicitation	8 - 10	7.3; 8.1 Factor 1 d)		Amendment 1 added an Organizational Conflict of Interest (OCI) Plan to the Factor 1 Staffing Plan to the Non-Price Volume of the proposal. Amendment 1 increased the Non-Price Volume of the proposal page limit from 7 to 9 and Amendment 2 increased it further from 9 to 12 pages. An effective OCI Plan that addresses the FAR requirements can easily exceed 12 pages by itself, especially when it includes forms for Non-Disclosure, Subcontractor Compliance, Documentation Handling/Labeling, etc. Will the government allow the OCI Plan to be excluded from the Non-Price Volume page limitations similar to Key Personnel Resumes, Relevant Experience Data Sheets and CPARS Evaluation Reports?	The Government believes the page limit is adequate, no revisions will be made.
2	2 and Q&A #35	All tabs except T&M Rate Table Tab	Rows 56-60		Amendment 2 changed the definitions of these rows to the following: Row 56 - Total T&M (Period) w/o CLIN 0005; Row 57 - Total T&M w/ potential options (Period); Row 58 - Total FFP Base Year; Row 59 - Total Period Value (All Options); and Row 60 - Total Contract Value All Options. Question 35 asked the government to provide formulas for rows 56 through 61. The government's answer stated "No please input your own formulas, as the form is editable the Government will not be responsible for incorrect pricing information." Unfortunately, there are various ways to interpret the descriptions of each row. Row 60 for Total Contract Value All Options is on each tab. There is no value of this line on each tab if it represents the Total Contract Value All Options as it would be the same number on each tab. If it means the Total Contract Value plus Options for each period, it makes sense to have this line on each tab however, there will not be a place in the workbook for Total Contract Value which summarizes each time period. How would the government like offerors to interpret each description for Rows 56 through 60?	Row 56 is all the T&M CLINs exclusive of the Optional Support under CLIN x005, essentially total T&M ceiling that would be put on contract initially x004, x006, x007 and x008. Row 57 would include CLIN x005 to depict the total potential T&M ceiling amount. Row 58 is all the FFP CLINs x001-x003. Row 59 is the total value for that Year (Base or Options 1-4). Row 60 will be the same across each spreadsheet and show the total contract value of all options.
3					Attachment 2 indicates that there is a single Lead CDM SME (Master) who is a Key personnel, who appears on Line 5. Attachment E shows the qualifications for this Key personnel, but includes a second CDM SME (Master) under Subtask 2.2 as a non-Key personnel on page 6. This second CDM SME (Master) does not appear on the pricing spreadsheet. We request clarification on this discrepancy from the Government.	The pricing spreadsheet is correct. Attachment E has been updated.